

JP 001 488

E K U
日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

06.07.00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2000年 4月21日

出願番号

Application Number:

特願2000-126305

出願人

Applicant (s):

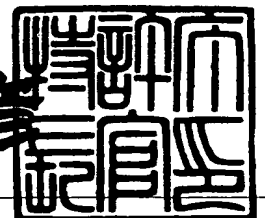
ソニー株式会社

**PRIORITY
DOCUMENT**SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 6月 9日

特許庁長官
Commissioner,
Patent Office

近藤 隆彦



出証番号 出証特2000-3043026

【書類名】 特許願

【整理番号】 0000438311

【提出日】 平成12年 4月21日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 野中 聡

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 江崎 正

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100094053

【弁理士】

【氏名又は名称】 佐藤 隆久

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第193562号

【出願日】 平成11年 7月 7日

【手数料の表示】

【予納台帳番号】 014890

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707389

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ提供システム、データ提供装置およびそれらの方法とデータ処理装置

【特許請求の範囲】

【請求項 1】

データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 2】

前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する

請求項 1 に記載のデータ提供システム。

【請求項 3】

前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置

をさらに有する請求項 2 に記載のデータ提供システム。

【請求項 4】

前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよ

び前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する請求項1に記載のデータ提供システム。

【請求項5】

前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項4に記載のデータ提供システム。

【請求項6】

前記公開鍵データの正当性を証明する公開鍵証明書データを作成する管理装置をさらに有し、

前記データ提供装置は、前記公開鍵証明書データを格納した前記モジュールを前記データ処理装置に配給する

請求項5に記載のデータ提供システム。

【請求項7】

前記データ提供装置は、

前記コンテンツデータを格納した第1のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第2のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項1に記載のデータ提供システム。

【請求項8】

前記データ提供装置は、前記第1のファイルおよび前記第2のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項7に記載のデータ提供システム。

【請求項9】

前記データ提供装置は、前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項8に記載のデータ提供システム。

【請求項 1 0】

前記データ提供装置は、前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項 1 に記載のデータ提供システム。

【請求項 1 1】

前記データ提供装置は、前記モジュールを記録した記録媒体を作成する

請求項 1 に記載のデータ提供システム。

【請求項 1 2】

前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する

請求項 1 に記載のデータ提供システム。

【請求項 1 3】

前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号化されたコンテンツデータとを復号装置に出力する

請求項 1 に記載のデータ提供システム。

【請求項 1 4】

前記データ処理装置は、前記モジュールに格納された公開鍵データを用いて、前記モジュールに格納された署名データの正当性を検証する

請求項 9 に記載のデータ提供システム。

【請求項 1 5】

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置の関係者に分配するための利益分配処理を行う

請求項 3 に記載のデータ提供システム。

【請求項 16】

前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる請求項 1 に記載のデータ提供システム。

【請求項 17】

データ提供装置から配給されたコンテンツデータを利用するデータ処理装置において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ提供装置から受けて、当該受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ処理装置。

【請求項 18】

データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 2 のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 1 9】

前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第 2 のモジュールを前記データ処理装置に配給する

請求項 1 8 に記載のデータ提供システム。

【請求項 2 0】

前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記第 1 のモジュールを前記データ配給装置に提供し、

前記データ処理装置は、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する

請求項 1 8 に記載のデータ提供システム。

【請求項 2 1】

前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置

をさらに有する請求項 2 0 に記載のデータ提供システム。

【請求項 2 2】

前記データ提供装置は、前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納し、前記配信用鍵データを用いて暗号化された第 3 のモジュールを格納した前記第 1 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第 3 のモジュールを前記第 2 のモジュールに格納して前記データ処理装置に配給する

請求項 2 0 に記載のデータ提供システム。

【請求項 2 3】

前記データ提供装置は、自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記第 3 のモジュールを格納した前記第 1 のモジュールを前記データ配給装置に提供する

請求項 2 2 に記載のデータ提供システム。

【請求項 2 4】

前記公開鍵データの正当性を証明する公開鍵証明書データを作成する管理装置をさらに有し、

前記データ提供装置は、前記公開鍵証明書データを格納した前記第 3 のモジュールを格納した前記第 1 のモジュールを前記データ配給装置に提供する請求項 2 3 に記載のデータ提供システム。

【請求項 2 5】

前記データ提供装置は、

前記コンテンツデータを格納した第 1 のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第 2 のファイルとを格納した前記第 1 のモジュールを前記データ配給装置に提供する

請求項 1 8 に記載のデータ提供システム。

【請求項 2 6】

前記データ提供装置は、前記第 1 のファイルおよび前記第 2 のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記第 1 のモジュールを前記データ配給装置に提供する

請求項 2 5 に記載のデータ提供システム。

【請求項 2 7】

前記データ提供装置は、前記秘密鍵データに対応する公開鍵データを格納した前記第 1 のモジュールを前記データ配給装置に提供する

請求項 2 5 に記載のデータ提供システム。

【請求項 2 8】

前記データ配給装置は、前記価格データに対して自らの秘密鍵データを用いて署名データを作成し、当該署名データを前記第 2 のモジュールに格納して前記データ処理装置に配給する

請求項 1 9 に記載のデータ提供システム。

【請求項 2 9】

前記データ提供装置は、前記自らの秘密鍵データに対応する公開鍵データを格納した前記第 2 のモジュールを前記データ処理装置に提供する

請求項 28 に記載のデータ提供システム。

【請求項 30】

前記データ配給装置は、前記第 1 のファイルおよび前記第 2 のファイルについての署名データを、前記データ提供装置の公開鍵データを用いて検証する
請求項 26 に記載のデータ提供システム。

【請求項 31】

前記データ提供装置は、

前記第 1 のファイルと、第 2 のファイルとのリンク関係を示すリンクデータを格納した前記第 1 のモジュールを前記データ配給装置に提供する

請求項 25 に記載のデータ提供システム。

【請求項 32】

前記データ配給装置は、前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記第 2 のモジュールを暗号化し、当該暗号化した第 2 のモジュールを前記データ処理装置に送信する

請求項 18 に記載のデータ提供システム。

【請求項 33】

前記データ配給装置は、前記モジュールを記録した記録媒体を作成する

請求項 18 に記載のデータ提供システム。

【請求項 34】

前記データ処理装置は、前記権利書データに基づいて、前記コンテンツデータの購入形態および利用形態の少なくとも一方を決定する

請求項 18 に記載のデータ提供システム。

【請求項 35】

前記データ処理装置は、前記復号したコンテンツ鍵データと、前記暗号化されたコンテンツデータとを復号装置に出力する

請求項 18 に記載のデータ提供システム。

【請求項 36】

前記データ処理装置は、前記第 2 のモジュールに格納された公開鍵データを用いて、前記第 2 のモジュールに格納された署名データの正当性を検証する

請求項 2 9 に記載のデータ提供システム。

【請求項 3 7】

前記データ処理装置は、前記権利書データに基づいて、前記配給を受けたコンテンツデータの購入形態および利用形態の少なくとも一方を決定し、当該決定した購入形態および利用形態の少なくとも一方の履歴を示す履歴データを前記管理装置に送信し、

前記管理装置は、受信した前記履歴データに基づいて、前記データ処理装置における前記コンテンツデータの前記購入および前記利用に伴って得られた利益を、前記データ提供装置および前記データ配給装置の関係者に分配するための利益分配処理を行う

請求項 2 1 に記載のデータ提供システム。

【請求項 3 8】

前記データ処理装置は、その処理内容、内部メモリに記憶された所定のデータおよび処理中のデータを、外部から監視および改竄困難なモジュールからなる

請求項 1 8 に記載のデータ提供システム。

【請求項 3 9】

データ提供装置と、少なくとも第 1 のデータ配給装置および第 2 のデータ配給装置と、データ処理装置とを有するデータ提供システムにおいて、

前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第 1 のモジュールを前記複数のデータ配給装置に提供し、

前記第 1 のデータ配給装置は、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 2 のモジュールを前記データ処理装置に配給し、

前記第 2 のデータ配給装置は、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 3 のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 2 のモジュールおよび前記第

3 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 4 0】

少なくとも第 1 のデータ提供装置および第 2 のデータ提供装置と、データ配給装置と、データ処理装置とを有するデータ提供システムにおいて、

前記第 1 のデータ提供装置は、第 1 のコンテンツ鍵データを用いて暗号化された第 1 のコンテンツデータと、暗号化された前記第 1 のコンテンツ鍵データと、前記第 1 のコンテンツデータの取り扱いを示す暗号化された第 1 の権利書データとを格納した第 1 のモジュールを前記データ配給装置に提供し、

前記第 2 のデータ提供装置は、第 2 のコンテンツ鍵データを用いて暗号化された第 2 のコンテンツデータと、暗号化された前記第 2 のコンテンツ鍵データと、前記第 2 のコンテンツデータの取り扱いを示す暗号化された第 2 の権利書データとを格納した第 2 のモジュールを前記データ配給装置に提供し、

前記データ配給装置は、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化された前記第 1 のコンテンツデータ、前記第 1 のコンテンツ鍵データおよび前記第 1 の権利書データと、前記提供を受けた前記第 2 のモジュールに格納された前記暗号化された前記第 2 のコンテンツデータ、前記第 2 のコンテンツ鍵データおよび前記第 2 の権利書データとを格納した第 3 のモジュールを前記データ処理装置に配給し、

前記データ処理装置は、前記配給を受けた前記第 3 のモジュールに格納された前記第 1 のコンテンツ鍵データおよび前記第 1 の権利書データを復号し、当該復号した第 1 の権利書データに基づいて、前記第 1 のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第 3 のモジュールに格納された前記第 2 のコンテンツ鍵データおよび前記第 2 の権利書データを復号し、当該復号した第 2 の権利書データに基づいて、前記第 2 のコンテンツデータの取り扱いを決定する

データ提供システム。

【請求項 4 1】

コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供装置において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給するデータ提供装置。

【請求項 4 2】

前記権利書データを作成、当該作成した権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 1 に記載のデータ提供装置。

【請求項 4 3】

配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 1 に記載のデータ提供装置。

【請求項 4 4】

所定の権威機関が発行した前記配信用鍵データを用いて、前記コンテンツ鍵データ K c および前記権利書データを暗号化する

請求項 4 3 に記載のデータ提供装置。

【請求項 4 5】

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 1 に記載のデータ提供装置。

【請求項 4 6】

自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項 4 5 に記載のデータ提供装置。

【請求項 47】

前記公開鍵データの正当性を証明する公開鍵証明書データを格納した前記モジュールを前記データ処理装置に配給する

請求項 46 に記載のデータ提供装置。

【請求項 48】

前記コンテンツデータを格納した第 1 のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第 2 のファイルとを格納した前記モジュールを前記データ処理装置に配給する

請求項 41 に記載のデータ提供装置。

【請求項 49】

前記第 1 のファイルおよび前記第 2 のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項 48 に記載のデータ提供装置。

【請求項 50】

前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項 49 に記載のデータ提供装置。

【請求項 51】

前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する

請求項 41 に記載のデータ提供装置。

【請求項 52】

前記モジュールを記録した記録媒体を作成する

請求項 41 に記載のデータ提供装置。

【請求項 53】

前記モジュールをアプリケーション層で定義する

請求項 41 に記載のデータ提供装置。

【請求項 5 4】

前記モジュールを前記データ処理装置に配給する配送プロトコルとして、前記アプリケーション層の下層のプレゼンテーション層およびトランスポート層を用いる

請求項 5 3 に記載のデータ提供装置。

【請求項 5 5】

前記モジュールを前記データ処理装置に配給するための媒体に依存しない形式で前記モジュールを定義する

請求項 4 1 に記載のデータ提供装置。

【請求項 5 6】

データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法において、

前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 5 7】

前記データ提供装置から前記データ処理装置に、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを配給し、

前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する

請求項 5 6 に記載のデータ提供方法。

【請求項 58】

データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを提供し、

前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 59】

前記データ配給装置から前記データ処理装置に、前記コンテンツデータの価格を示す価格データを格納した前記第2のモジュールを配給する

請求項 58 に記載のデータ提供方法。

【請求項 60】

データ提供装置と、少なくとも第1のデータ配給装置および第2のデータ配給装置と、データ処理装置とを用いたデータ提供方法において、

前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを提供し、

前記第1のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを配給し、

前記第2のデータ配給装置から前記データ処理装置に、前記提供を受けた前記

第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 3 のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第 2 のモジュールおよび前記第 3 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する

データ提供方法。

【請求項 6 1】

少なくとも第 1 のデータ提供装置および第 2 のデータ提供装置と、データ配給装置と、データ処理装置とを用いたデータ提供方法において、

前記第 1 のデータ提供装置から前記データ配給装置に、第 1 のコンテンツ鍵データを用いて暗号化された第 1 のコンテンツデータと、暗号化された前記第 1 のコンテンツ鍵データと、前記第 1 のコンテンツデータの取り扱いを示す暗号化された第 1 の権利書データとを格納した第 1 のモジュールを提供し、

前記第 2 のデータ提供装置から前記データ配給装置に、第 2 のコンテンツ鍵データを用いて暗号化された第 2 のコンテンツデータと、暗号化された前記第 2 のコンテンツ鍵データと、前記第 2 のコンテンツデータの取り扱いを示す暗号化された第 2 の権利書データとを格納した第 2 のモジュールを提供し、

前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化された前記第 1 のコンテンツデータ、前記第 1 のコンテンツ鍵データおよび前記第 1 の権利書データと、前記提供を受けた前記第 2 のモジュールに格納された前記暗号化された前記第 2 のコンテンツデータ、前記第 2 のコンテンツ鍵データおよび前記第 2 の権利書データとを格納した第 3 のモジュールを配給し、

前記データ処理装置において、前記配給を受けた前記第 3 のモジュールに格納された前記第 1 のコンテンツ鍵データおよび前記第 1 の権利書データを復号し、当該復号した第 1 の権利書データに基づいて、前記第 1 のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第 3 のモジュールに格納された前記第 2 のコンテンツ鍵データおよび前記第 2 の権利書データを復号し、当該復号した第

2の権利書データに基づいて、前記第2のコンテンツデータの取り扱いを決定する

データ提供方法。

【請求項62】

コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供方法において、

コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給する

データ提供方法。

【請求項63】

配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給する

請求項62に記載のデータ提供方法。

【請求項64】

前記コンテンツデータ、前記コンテンツ鍵データおよび前記権利書データの少なくとも一つに対して自らの署名データを作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する

請求項62に記載のデータ提供方法。

【請求項65】

自らの秘密鍵データを用いて前記署名データを作成し、当該秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する

請求項64に記載のデータ提供方法。

【請求項66】

前記公開鍵データの正当性を証明する公開鍵証明書データを格納した前記モジュールを前記データ処理装置に配給する

請求項65に記載のデータ提供方法。

【請求項67】

前記コンテンツデータを格納した第1のファイルと、

前記コンテンツ鍵データおよび前記権利書データを格納した第2のファイルとを格納した前記モジュールを前記データ処理装置に配給する
請求項62に記載のデータ提供方法。

【請求項68】

前記第1のファイルおよび前記第2のファイルについて、自らの秘密鍵データを用いた署名データをそれぞれ作成し、当該作成した署名データを格納した前記モジュールを前記データ処理装置に配給する
請求項67に記載のデータ提供方法。

【請求項69】

前記秘密鍵データに対応する公開鍵データを格納した前記モジュールを前記データ処理装置に配給する
請求項68に記載のデータ提供方法。

【請求項70】

前記データ処理装置との間で相互認証を行い、当該相互認証によって得たセッション鍵データを用いて前記モジュールを暗号化し、当該暗号化したモジュールを前記データ処理装置に送信する
請求項62に記載のデータ提供方法。

【請求項71】

前記モジュールを記録した記録媒体を作成する
請求項62に記載のデータ提供方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンテンツデータを提供するデータ提供システム、データ提供装置およびそれらの方法とデータ処理装置に関する。

【0002】

【従来の技術】

暗号化されたコンテンツデータを所定の契約を交わしたユーザのデータ処理装置に配給し、当該データ処理装置において、コンテンツデータを復号して再生お

よび記録するデータ提供システムがある。

このようなデータ提供システムの一つに、音楽データを配信する従来のEMD (Electronic Music Distribution: 電子音楽配信) システムがある。

【0003】

図100は、従来のEMDシステム700の構成図である。

図100に示すEMDシステム700では、コンテンツプロバイダ701a, 701bが、サービスプロバイダ710に対し、コンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとを、それぞれ相互認証後に得たセッション鍵データで暗号化してオンラインで供給したり、あるいはオフラインで供給する。ここで、著作権情報705a, 705b, 705cには、例えば、SCMS (Serial Copy Management System) 情報、コンテンツデータに埋め込むことを要請する電子透かし情報およびサービスプロバイダ710の伝送プロトコルに埋め込むことを要請する著作権に関する情報などがある。

【0004】

サービスプロバイダ710は、受信したコンテンツデータ704a, 704b, 704cと、著作権情報705a, 705b, 705cとをセッション鍵データを用いて復号する。

そして、サービスプロバイダ710は、復号したあるいはオフラインで受け取ったコンテンツデータ704a, 704b, 704cに、著作権情報705a, 705b, 705cを埋め込んで、コンテンツデータ707a, 707b, 707cを生成する。このとき、サービスプロバイダ710は、例えば、著作権情報705a, 705b, 705cのうち電子透かし情報をコンテンツデータ704a, 704b, 704cに所定の周波数領域を変更して埋め込み、当該コンテンツデータをユーザに送信する際に用いるネットワークプロトコルにSCMS情報を埋め込む。

さらに、サービスプロバイダ710は、コンテンツデータ707a, 707b, 707cを、鍵データベース706から読み出したコンテンツ鍵データKca, Kcb, Kccを用いてそれぞれ暗号化する。その後、サービスプロバイダ710は、暗号化されたコンテンツデータ707a, 707b, 707cを格納し

たセキュアコンテナ722を、相互認証後に得たセッション鍵データによって暗号化してユーザの端末装置709に存在するCA (Conditional Access) モジュール711に送信する。

【0005】

CAモジュール711は、セキュアコンテナ722をセッション鍵データを用いて復号する。また、CAモジュール711は、電子決済やCAなどの課金機能を用いて、サービスプロバイダ710の鍵データベース706からコンテンツ鍵データKca, Kcb, Kccを受信し、これをセッション鍵データを用いて復号する。これにより、端末装置709において、コンテンツデータ707a, 707b, 707cを、それぞれコンテンツ鍵データKca, Kcb, Kccを用いて復号することが可能になる。

このとき、CAモジュール711は、コンテンツ単位で課金処理を行い、その結果に応じた課金情報721を生成し、これをセッション鍵データで暗号化した後に、サービスプロバイダ710の権利処理モジュール720に送信する。

この場合に、CAモジュール711は、サービスプロバイダ710が自らの提供するサービスに関して管理したい項目であるユーザの契約（更新）情報および月々基本料金などのネットワーク家賃の徴収と、コンテンツ単位の課金処理と、ネットワークの物理層のセキュリティ確保とを行う。

【0006】

サービスプロバイダ710は、CAモジュール711から課金情報721を受信すると、サービスプロバイダ710とコンテンツプロバイダ701a, 701b, 701cとの間で利益配分を行う。

このとき、サービスプロバイダ710から、コンテンツプロバイダ701a, 701b, 701cへの利益配分は、例えば、JASRAC (Japanese Society for Rights of Authors, Composers and Publishers: 日本音楽著作権協会) を介して行われる。また、JASRACによって、コンテンツプロバイダの利益が、当該コンテンツデータの著作権者、アーティスト、作詞・作曲家および所属プロダクションなどに分配される。

【0007】

また、端末装置709では、コンテンツ鍵データKca, Kcb, Kccを用いて復号したコンテンツデータ707a, 707b, 707cを、RAM型の記録媒体723などに記録する際に、著作権情報705a, 705b, 705cのSCMSビットを書き換えて、コピー制御を行う。すなわち、ユーザ側では、コンテンツデータ707a, 707b, 707cに埋め込まれたSCMSビットに基づいて、コピー制御が行われ、著作権の保護が図られている。

【0008】

【発明が解決しようとする課題】

ところで、SCMSは、CD(Compact Disc)からDAT(Digital Audio Tape)への録音を防止するために規定されたものであり、DATとDATとの間での複製が可能である。また、コンテンツデータに電子透かし情報を埋め込んだ場合も、問題が生じたときに、対象となっているコンテンツデータを提供したコンテンツプロバイダを特定するに止まり、違法なコピーを技術的に阻止するものではない。

従って、上述した図100に示すEMDシステム700では、コンテンツプロバイダの権利(利益)が十分に保護されないという問題がある。

【0009】

また、上述したEMDシステム700では、コンテンツプロバイダの著作権情報をサービスプロバイダがコンテンツデータに埋め込むため、コンテンツプロバイダは当該埋め込みが要求通りに行われているかを監査する必要がある。また、コンテンツプロバイダは、サービスプロバイダが契約通りに、コンテンツデータの配信を行っているかを監査する必要がある。そのため、監査のための負担が大きいという問題がある。

【0010】

また、上述したEMDシステム700では、ユーザの端末装置709からの課金情報721を、サービスプロバイダ710の権利処理モジュール720で処理するため、ユーザによるコンテンツデータの利用に応じてコンテンツプロバイダが受けるべき利益を、コンテンツプロバイダが適切に受けられるかどうか懸念

される。

【 0 0 1 1 】

本発明は上述した従来技術の問題点に鑑みてなされ、コンテンプロバイダの権利者（関係者）の利益を適切に保護できるデータ提供システム、データ提供装置およびそれらの方法とデータ処理装置とを提供することを目的とする。

また、本発明は、コンテンプロバイダの権利者の利益を保護するための監査の負担を軽減できるデータ提供システム、データ提供装置およびそれらの方法とデータ処理装置とを提供することを目的とする。

【 0 0 1 2 】

【課題を解決するための手段】

上述した従来技術の問題点を解決し、上述した目的を達成するために、本発明の第 1 の観点のデータ提供システムは、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【 0 0 1 3 】

本発明の第 1 の観点のデータ提供システムでは、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールが配給される。

そして、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

このように、コンテンツデータを格納したモジュールに、当該コンテンツデータの取り扱いを示す権利書データを格納することで、データ処理装置において、

データ提供装置の関係者が作成した権利書データに基づいたコンテンツデータの取り扱い（利用）を行わせることが可能になる。

【0014】

また、本発明の第1の観点のデータ提供システムは、好ましくは、前記データ提供装置は、配信用鍵データを用いてそれぞれ暗号化された前記コンテンツ鍵データおよび前記権利書データを格納した前記モジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを前記配信用鍵データを用いて復号する。

【0015】

また、本発明の第1の観点のデータ提供システムは、好ましくは、前記配信用鍵データを管理し、前記データ提供装置および前記データ処理装置に前記配信用鍵データを配給する管理装置をさらに有する。

【0016】

また、本発明のデータ処理装置は、データ提供装置から配給されたコンテンツデータを利用するデータ処理装置であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ提供装置から受けて、当該受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0017】

また、本発明の第2の観点のデータ提供システムは、データ提供装置、データ配給装置およびデータ処理装置を有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利

書データを格納した第2のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0018】

本発明の第2の観点のデータ提供システムでは、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールが提供される。

次に、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールが配給される。

次に、前記データ処理装置において、前記配給を受けた前記第2のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データが復号され、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いが決定される。

【0019】

また、本発明の第2の観点のデータ提供システムは、好ましくは、前記データ配給装置は、前記コンテンツデータの価格を示す価格データを格納した前記第2のモジュールを前記データ処理装置に配給する。

【0020】

また、本発明の第3の観点のデータ提供システムは、データ提供装置と、少なくとも第1のデータ配給装置および第2のデータ配給装置と、データ処理装置とを有するデータ提供システムであって、前記データ提供装置は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを前記複数のデータ配給装置に提供し、前記第1のデータ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納し

た第2のモジュールを前記データ処理装置に配給し、前記第2のデータ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第3のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第2のモジュールおよび前記第3のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【 0 0 2 1 】

また、本発明の第4の観点のデータ提供システムは、少なくとも第1のデータ提供装置および第2のデータ提供装置と、データ配給装置と、データ処理装置とを有するデータ提供システムであって、前記第1のデータ提供装置は、第1のコンテンツ鍵データを用いて暗号化された第1のコンテンツデータと、暗号化された前記第1のコンテンツ鍵データと、前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のモジュールを前記データ配給装置に提供し、前記第2のデータ提供装置は、第2のコンテンツ鍵データを用いて暗号化された第2のコンテンツデータと、暗号化された前記第2のコンテンツ鍵データと、前記第2のコンテンツデータの取り扱いを示す暗号化された第2の権利書データとを格納した第2のモジュールを前記データ配給装置に提供し、前記データ配給装置は、前記提供を受けた前記第1のモジュールに格納された前記暗号化された前記第1のコンテンツデータ、前記第1のコンテンツ鍵データおよび前記第1の権利書データと、前記提供を受けた前記第2のモジュールに格納された前記暗号化された前記第2のコンテンツデータ、前記第2のコンテンツ鍵データおよび前記第2の権利書データとを格納した第3のモジュールを前記データ処理装置に配給し、前記データ処理装置は、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データおよび前記第1の権利書データを復号し、当該復号した第1の権利書データに基づいて、前記第1のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第3のモジュールに格納された前記第2のコンテンツ鍵データおよび前記第2の権利書データを復号し、当該復号した第2の権利書データに基づいて、前記第2のコンテンツデータの

取り扱いを決定する。

【 0 0 2 2 】

また、本発明のデータ提供装置は、コンテンツデータの利用を行うデータ処理装置に、前記コンテンツデータを配給するデータ提供装置であって、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを前記データ処理装置に配給する。

【 0 0 2 3 】

また、本発明の第 1 の観点のデータ提供方法は、データ提供装置からデータ処理装置にコンテンツデータを配給するデータ提供方法であって、前記データ提供装置から前記データ処理装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したモジュールを配給し、前記データ処理装置において、前記配給を受けた前記モジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【 0 0 2 4 】

また、本発明の第 2 の観点のデータ提供方法は、データ提供装置、データ配給装置およびデータ処理装置を用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第 1 のモジュールを提供し、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第 1 のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第 2 のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第 2 のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0025】

また、本発明の第3の観点のデータ提供方法は、データ提供装置と、少なくとも第1のデータ配給装置および第2のデータ配給装置と、データ処理装置とを用いたデータ提供方法であって、前記データ提供装置から前記データ配給装置に、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、暗号化された前記コンテンツ鍵データと、前記コンテンツデータの取り扱いを示す暗号化された権利書データとを格納した第1のモジュールを提供し、前記第1のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第2のモジュールを配給し、前記第2のデータ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化されたコンテンツデータ、コンテンツ鍵データおよび権利書データを格納した第3のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第2のモジュールおよび前記第3のモジュールに格納された前記コンテンツ鍵データおよび前記権利書データを復号し、当該復号した権利書データに基づいて、前記コンテンツデータの取り扱いを決定する。

【0026】

また、本発明の第4の観点のデータ提供方法は、少なくとも第1のデータ提供装置および第2のデータ提供装置と、データ配給装置と、データ処理装置とを用いたデータ提供方法であって、前記第1のデータ提供装置から前記データ配給装置に、第1のコンテンツ鍵データを用いて暗号化された第1のコンテンツデータと、暗号化された前記第1のコンテンツ鍵データと、前記第1のコンテンツデータの取り扱いを示す暗号化された第1の権利書データとを格納した第1のモジュールを提供し、前記第2のデータ提供装置から前記データ配給装置に、第2のコンテンツ鍵データを用いて暗号化された第2のコンテンツデータと、暗号化された前記第2のコンテンツ鍵データと、前記第2のコンテンツデータの取り扱いを示す暗号化された第2の権利書データとを格納した第2のモジュールを提供し、前記データ配給装置から前記データ処理装置に、前記提供を受けた前記第1のモジュールに格納された前記暗号化された前記第1のコンテンツデータ、前記第1

のコンテンツ鍵データおよび前記第1の権利書データと、前記提供を受けた前記第2のモジュールに格納された前記暗号化された前記第2のコンテンツデータ、前記第2のコンテンツ鍵データおよび前記第2の権利書データとを格納した第3のモジュールを配給し、前記データ処理装置において、前記配給を受けた前記第3のモジュールに格納された前記第1のコンテンツ鍵データおよび前記第1の権利書データを復号し、当該復号した第1の権利書データに基づいて、前記第1のコンテンツデータの取り扱いを決定し、前記配給を受けた前記第3のモジュールに格納された前記第2のコンテンツ鍵データおよび前記第2の権利書データを復号し、当該復号した第2の権利書データに基づいて、前記第2のコンテンツデータの取り扱いを決定する。

【0027】

【発明の実施の形態】

以下、本発明の実施形態に係わるEMD(Electronic Music Distribution: 電子音楽配信)システムについて説明する。

本実施形態において、ユーザに配信されるコンテンツ(Content)データとは、音楽データ、映像データおよびプログラムなど情報そのものが価値を有するデジタルデータをいい、以下、音楽データを例に説明する。

【0028】

第1実施形態

図1は、本実施形態のEMDシステム100の構成図である。

図1に示すように、EMDシステム100は、コンテンツプロバイダ101、EMDサービスセンタ(クリアリング・ハウス、以下、ESCとも記す)102およびユーザホームネットワーク103を有する。

ここで、コンテンツプロバイダ101、EMDサービスセンタ102およびSAM105₁～105₄が、それぞれ請求項1および請求項3などに係わるデータ提供装置、管理装置およびデータ処理装置に対応している。

まず、EMDシステム100の概要について説明する。

EMDシステム100では、コンテンツプロバイダ101は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す

権利書(UCP:Usage Control Policy)データ106を、高い信頼性のある権威機関であるEMDサービスセンタ102に送信する。権利書データ106は、EMDサービスセンタ102によって権威化(認証)される。

【0029】

また、コンテンツプロバイダ101は、コンテンツ鍵データKcでコンテンツデータCを暗号化してコンテンツファイルCFを生成すると共に、コンテンツ鍵データKcをEMDサービスセンタ102から配給された対応する期間の配信用鍵データKD₁～KD₅₆で暗号化する。そして、コンテンツプロバイダ101は、暗号化されたコンテンツ鍵データKcおよびコンテンツファイルCFと自らの署名データとを格納(カプセル化)したセキュアコンテナ(本発明のモジュール)104を、インターネットなどのネットワーク、デジタル放送あるいは記録媒体などを用いて、ユーザホームネットワーク103に配給する。

このように、本実施形態では、デジタルのコンテンツデータCをカプセル化して提供することで、従来の記録媒体と密着したデジタルコンテンツを、記録媒体から切り離して、デジタルコンテンツ単体に存在価値を持たせることができる。

ここで、セキュアコンテナは、どのような流通経路(配送チャンネル)を介して提供されても、コンテンツデータC(商品)を販売するときの最も基本となる商品カプセルである。具体的には、セキュアコンテナは、課金を行うための暗号情報や、コンテンツデータCの中身の正当性、コンテンツデータを作成した者の正当性およびコンテンツデータの流通業者の正当性を検証するための署名データや、コンテンツデータに埋め込む電子透かし情報に関する情報などの著作権に係わる情報を含む商品カプセルである。

【0030】

ユーザホームネットワーク103は、例えば、ネットワーク機器160₁およびAV機器160₂～160₄を有する。

ネットワーク機器160₁は、SAM(Secure Application Module)105₁を内蔵している。

AV機器160₂～160₄は、それぞれSAM105₂～105₄を内蔵している。SAM105₁～105₄相互間は、例えば、IEEE(Institute of

Electrical and Electronics Engineers) 1394 シリアルインタフェースバスなどのバス191を介して接続されている。

【0031】

SAM105₁ ~ 105₄ は、ネットワーク機器160₁ がコンテンツプロバイダ101からネットワークなどを介してオンラインで受信したセキュアコンテナ104、および／または、コンテンツプロバイダ101からAV機器160₂ ~ 160₄ に記録媒体を介してオフラインで供給されたセキュアコンテナ104を対応する期間の配信用鍵データKD₁ ~ KD₃ を用いて復号した後に、署名データの検証を行う。

SAM105₁ ~ 105₄ に供給されたセキュアコンテナ104は、ネットワーク機器160₁ およびAV機器160₂ ~ 160₄ において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

SAM105₁ ~ 105₄ は、上述したセキュアコンテナ104の購入・利用の履歴を利用履歴(Usage Log) データ108として記録する。

利用履歴データ108は、例えば、EMDサービスセンタ102からの要求に応じて、ユーザホームネットワーク103からEMDサービスセンタ102に送信される。

【0032】

EMDサービスセンタ102は、利用履歴データ108に基づいて、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが決済機関91に支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101に支払われる。

また、EMDサービスセンタ102は、一定期間毎に、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0033】

本実施形態では、EMDサービスセンタ102は、認証機能、鍵データ管理機能および権利処理(利益分配)機能を有している。

すなわち、EMDサービスセンタ102は、中立の立場にある最高の権威機関であるルート認証局92に対しての（ルート認証局92の下層に位置する）セカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ101およびSAM105₁～105₄において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ102の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、EMDサービスセンタ102は、コンテンツプロバイダ101の権利書データ106を登録して権威化すること、EMDサービスセンタ102の認証機能の一つである。

また、EMDサービスセンタ102は、例えば、配信用鍵データKD₁～KD₆などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMDサービスセンタ102は、権威化した権利書データ106に記述された標準小売価格SRP(Suggested Retailer' Price)とSAM105₁～SAM105₄から入力した利用履歴データ108とに基づいて、ユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ101に分配する権利処理（利益分配）機能を有する。

【0034】

以下、コンテンツプロバイダ101の各構成要素について詳細に説明する。

【コンテンツプロバイダ101】

図2は、コンテンツプロバイダ101の機能ブロック図であり、ユーザホームネットワーク103のSAM105₁～105₄との間で送受信されるデータに関連するデータの流れが示されている。

また、図3には、コンテンツプロバイダ101とEMDサービスセンタ102との間で送受信されるデータに関連するデータの流れが示されている。

なお、図3以降の図面では、署名データ処理部、および、セッション鍵データK_{SES}を用いた暗号化・復号部に入出力するデータの流れは省略している。

【0035】

図2および図3に示すように、コンテンツプロバイダ101は、コンテンツマスタソースサーバ111、電子透かし情報付加部112、圧縮部113、暗号化

部 1 1 4、乱数発生部 1 1 5、暗号化部 1 1 6、署名処理部 1 1 7、セキュアコンテンツ作成部 1 1 8、セキュアコンテンツデータベース 1 1 8 a、記憶部 1 1 9、相互認証部 1 2 0、暗号化・復号部 1 2 1、権利書データ作成部 1 2 2、SAM 管理部 1 2 4 および EMD サービスセンタ管理部 1 2 5 を有する。

コンテンツプロバイダ 1 0 1 は、EMD サービスセンタ 1 0 2 との間で通信を行う前に、例えば、自らが生成した公開鍵データ、自らの身分証明書および銀行口座番号（決済を行う口座番号）をオフラインで EMD サービスセンタ 1 0 2 に登録し、自らの識別子（識別番号）CP_ID を得る。また、コンテンツプロバイダ 1 0 1 は、EMD サービスセンタ 1 0 2 から、EMD サービスセンタ 1 0 2 の公開鍵データと、ルート認証局 9 2 の公開鍵データとを受ける。

以下、図 2 および図 3 に示すコンテンツプロバイダ 1 0 1 の各機能ブロックについて説明する。

【 0 0 3 6 】

コンテンツマスターソースサーバ 1 1 1 は、ユーザホームネットワーク 1 0 3 に提供するコンテンツのマスターソースであるコンテンツデータを記憶し、提供しようとするコンテンツデータ S 1 1 1 を電子透かし情報付加部 1 1 2 に出力する。

【 0 0 3 7 】

電子透かし情報付加部 1 1 2 は、コンテンツデータ S 1 1 1 に対して、ソース電子透かし情報 (Source Watermark) W s、コピー管理用電子透かし情報 (Copy Control Watermark) W c およびユーザ電子透かし情報 (User Watermark) W u など を埋め込んでコンテンツデータ S 1 1 2 を生成し、コンテンツデータ S 1 1 2 を圧縮部 1 1 3 に出力する。

【 0 0 3 8 】

ソース電子透かし情報 W s は、コンテンツデータの著作権者名、I S R C コード、オーサリング日付、オーサリング機器 I D (Identification Data)、コンテンツの配給先などの著作権に関する情報である。コピー管理用電子透かし情報 W c は、アナログインタフェース経由でのコピー防止用のためのコピー禁止ビットを含む情報である。ユーザ電子透かし情報 W u には、例えば、セキュアコンテンツ 1 0 4 の配給元および配給先を特定するためのコンテンツプロバイダ 1 0 1 の識

別子CP_IDおよびユーザホームネットワーク103のSAM105₁~105₄の識別子SAM_ID₁~SAM_ID₄が含まれる。

また、電子透かし情報付加部112は、必要であれば、検索エンジンでコンテンツデータの検索を行うためのリンク用のIDを電子透かし情報としてコンテンツデータS111に埋め込む。

本実施形態では、好ましくは、各々の電子透かし情報の情報内容と埋め込み位置とを、電子透かし情報管理データとして定義し、EMDサービスセンタ102において電子透かし情報管理データを管理する。電子透かし情報管理データは、例えば、ユーザホームネットワーク103内のネットワーク機器160₁およびAV機器160₂~160₄が、電子透かし情報の正当性を検証する際に用いられる。

例えば、ユーザホームネットワーク103では、電子透かし情報管理データに基づいて、電子透かし情報の埋め込み位置および埋め込まれた電子透かし情報の内容の双方が一致した場合に電子透かし情報が正当であると判断することで、偽りの電子透かし情報の埋め込みを高い確率で検出できる。

【0039】

圧縮部113は、コンテンツデータS112を、例えば、ATRAC3(Adaptive Transform Acoustic Coding 3)(商標)などの音声圧縮方式で圧縮し、圧縮したコンテンツデータS113を暗号化部114に出力する。

【0040】

暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、DES(Data Encryption Standard)やTriple DESなどの共通鍵暗号化方式で、コンテンツデータS113を暗号化してコンテンツデータCを生成し、これをセキュアコンテナ作成部118に出力する。

また、暗号化部114は、コンテンツ鍵データKcを共通鍵として用い、A/V伸長用ソフトウェアSoftおよびメタデータMetaを暗号化した後に、セキュアコンテナ作成部117に出力する。

【0041】

DESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして

処理する暗号化方式である。DESの処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）データを共通鍵データから生成する部分（鍵処理部）とからなる。DESの全てのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【0042】

まず、平文の64ビットは、上位32ビットの H_0 と下位32ビットの L_0 とに分割される。鍵処理部から供給された48ビットの拡大鍵データ K_1 および下位32ビットの L_0 を入力とし、下位32ビットの L_0 を攪拌したF関数の出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットの H_0 と、F関数の出力との排他的論理和が算出され、その結果は L_1 とされる。また、 L_0 は、 H_1 とされる。

そして、上位32ビットの H_0 および下位32ビットの L_0 を基に、以上の処理を16回繰り返し、得られた上位32ビットの H_{16} および下位32ビットの L_{16} が暗号文として出力される。復号は、暗号化に使用した共通鍵データを用いて、上記の手順を逆さにたどることで実現される。

【0043】

乱数発生部115は、所定ビット数の乱数を発生し、当該乱数をコンテンツ鍵データ K_c として暗号化部114および暗号化部116に出力する。

なお、コンテンツ鍵データ K_c は、コンテンツデータが提供する楽曲に関する情報から生成してもよい。コンテンツ鍵データ K_c は、例えば、所定時間毎に更新される。

【0044】

暗号化部116は、後述するようにしてEMDサービスセンタ102から受信されて記憶部119に記憶された配信用鍵データ $KD_1 \sim KD_6$ のうち対応する期間の配信用鍵データ $KD_1 \sim KD_6$ を入力し、当該配信用鍵データを共通鍵として用いたDESなどの共通暗号化方式によって図4（B）に示すコンテンツ鍵データ K_c 、権利書データ106、SAMプログラム・ダウンロード・コンテナ

SDC₁ ~ SDC₃ および署名・証明書モジュールMod₁ を暗号化した後に、セキュアコンテナ作成部117に出力する。

署名・証明書モジュールMod₁ には、図4 (B) に示すように、署名データSIG_{2,CP} ~ SIG_{4,CP}、コンテンツプロバイダ101の公開鍵データK_{CP,P}の公開鍵証明書CER_{CP}および当該公開鍵証明書CER_{CP}に対してのEMDサービスセンタ102の署名データSIG_{1,ESC} が格納されている。

また、SAMプログラム・ダウンロード・コンテナSDC₁ ~ SDC₃ は、SAM105₁ ~ 105₄ 内でプログラムのダウンロードを行なう際に用いられるダウンロード・ドライバと、権利書データ(UCP) U106のシンタックス(文法)を示すUCP-L(Label) . R(Reader)と、SAM105₁ ~ 105₄ に内蔵された記憶部(フラッシュ-ROM)の書き換えおよび消去をブロック単位でロック状態/非ロック状態にするためのロック鍵データとを格納している。

【0045】

なお、記憶部119は、例えば、公開鍵証明書データを記憶するデータベース、配信用鍵データKD₁ ~ KD₆ を記憶するデータベースおよびキーファイルKFを記憶するデータベースなどの種々のデータベースを備えている。

【0046】

署名処理部117は、署名を行なう対象となるデータのハッシュ値をとり、コンテンツプロバイダ101の秘密鍵データK_{CP,S}を用いて、その署名データSIGを作成する。

【0047】

なお、ハッシュ値は、ハッシュ関数を用いて生成される。ハッシュ関数は、対象となるデータを入力とし、当該入力したデータを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値(出力)から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難であるという特徴を有している。

【0048】

セキュアコンテナ作成部118は、図4 (A) に示すように、ヘッダデータと

、暗号化部 114 から入力したそれぞれコンテンツ鍵データ K_c で暗号化されたコンテンツデータ C 、A/V 伸長用ソフトウェア $Soft$ およびメタデータ $Meta$ とを格納したコンテンツファイル CF を生成する。

ここで、A/V 伸長用ソフトウェア $Soft$ は、ユーザホームネットワーク 103 のネットワーク機器 160_1 および AV 機器 $160_2 \sim 160_4$ において、コンテンツファイル CF を伸長する際に用いられるソフトウェアであり、例えば、ATRAC3 方式の伸長用ソフトウェアである。

【0049】

また、セキュアコンテナ作成部 118 は、図 4 (B) に示すように、暗号化部 116 から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_6$ で暗号化されたコンテンツ鍵データ K_c 、権利書データ (UCP) 106 および SAM プログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ および署名・証明書モジュール Mod_1 を格納したキーファイル KF を生成する。

そして、セキュアコンテナ作成部 118 は、図 4 (A), (B) に示すコンテンツファイル CF およびキーファイル KF と、図 4 (C) に示すコンテンツプロバイダ 101 の公開鍵データ K_{CP} および署名データ $SIG_{1,ESC}$ とを格納したセキュアコンテナ 104 を生成し、これをセキュアコンテナデータバス 118a に格納した後に、ユーザからの要求に応じて SAM 管理部 124 に出力する。

このように、本実施形態では、コンテンツプロバイダ 101 の公開鍵データ $K_{CP,P}$ の公開鍵証明書 CER_{CP} をセキュアコンテナ 104 に格納してユーザホームネットワーク 103 に送信するイン・バンド (In-band) 方式を採用している。従って、ユーザホームネットワーク 103 は、公開鍵証明書 CER_{CP} を得るための通信を EMD サービスセンタ 102 との間で行う必要がない。

なお、本発明では、公開鍵証明書 CER_{CP} をセキュアコンテナ 104 に格納しないで、ユーザホームネットワーク 103 が EMD サービスセンタ 102 から公開鍵証明書 CER_{CP} を得るアウト・オブ・バンド (Out-Of-band) 方式を採用してもよい。

【0050】

相互認証部 120 は、コンテンツプロバイダ 101 が EMD サービスセンタ 1

02およびユーザホームネットワーク103との間でオンラインでデータを送受信する際に、それぞれEMDサービスセンタ102およびユーザホームネットワーク103との間で相互認証を行ってセッション鍵データ（共有鍵） K_{SES} を生成する。セッション鍵データ K_{SES} は、相互認証を行う度に新たに生成される。

【0051】

暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103にオンラインで送信するデータを、セッション鍵データ K_{SES} を用いて暗号化する。

また、暗号化・復号部121は、コンテンツプロバイダ101がEMDサービスセンタ102およびユーザホームネットワーク103からオンラインで受信したデータを、セッション鍵データ K_{SES} を用いて復号する。

【0052】

権利書データ作成部122は、権利書データ106を作成し、これを暗号化部116に出力する。

権利書データ106は、コンテンツデータCの運用ルールを定義した記述子（ディスクリプター）であり、例えば、コンテンツプロバイダ101の運用者が希望する標準小売価格SRP (Suggested Retailer' Price) やコンテンツデータCの複製ルールなどが記述されている。

【0053】

SAM管理部124は、セキュアコンテナ104を、オフラインおよび／またはオンラインでユーザホームネットワーク103に供給する。

SAM管理部124は、CD-ROMやDVD (Digital Versatile Disc)などのROM型の記録媒体（メディア）を用いてセキュアコンテナ104をオフラインでユーザホームネットワーク103に配給する場合には、配信用鍵データ $KD_1 \sim KD_6$ などを用いてセキュアコンテナ104を暗号化して記録媒体に記録する。そして、この記録媒体は、販売などにより、ユーザホームネットワーク103にオフラインで供給される。

【0054】

本実施形態では、セキュアコンテナ（商品カプセル）104は、図5に示すよ

うに、OSIレイヤ層におけるアプリケーション層で定義される。また、プレゼンテーション層やトランスポート層に相当するカプセルは、セキュアコンテナを配送するための配送プロトコルとして、セキュアコンテナ104とは別に定義される。従って、セキュアコンテナ104を配送プロトコルに依存しないで定義できる。すなわち、セキュアコンテナ104を、例えばオンラインおよびオフラインの何れの形態でユーザホームネットワーク103に供給する場合でも、共通のルールに従って定義および生成できる。

例えば、セキュアコンテナ104をネットワークを使って供給する場合には、セキュアコンテナ104をコンテンツプロバイダ101の領域で定義し、プレゼンテーション層およびトランスポート層をセキュアコンテナ104をユーザホームネットワーク103まで搬送するための搬送ツールと考える。

また、オフラインの場合に、ROM型の記録媒体を、セキュアコンテナ104をユーザホームネットワーク103に搬送する搬送キャリアとして考える。

【0055】

図6は、ROM型の記録媒体130を説明するための図である。

図6に示すように、ROM型の記録媒体130は、ROM領域131、RAM領域132およびメディアSAM133を有する。

ROM領域131には、図4(A)に示したコンテンツファイルCFが記憶されている。

また、RAM領域132には、図4(B)、(C)に示したキーファイルKFおよび公開鍵証明書データ $CE R_{CP}$ と機器の種類に応じて固有の値を持つ記録用鍵データ K_{STR} とを引数としてMAC(Message Authentication Code)関数を用いて生成したと署名データと、当該キーファイルKFおよび公開鍵証明書データ $CE R_{CP}$ とを記録媒体に固有の値を持つメディア鍵データ K_{MED} を用いて暗号化したデータとが記憶される。

また、RAM領域132には、例えば、不正行為などで無効となったコンテンツプロバイダ101およびSAM105₁～105₅を特定する公開鍵証明書破棄データ(リボケーションリスト)が記憶される。

また、また、RAM領域132には、後述するようにユーザホームネットワー

ク103のSAM105₁～105₄においてコンテンツデータCの購入・利用形態が決定されたときに生成される利用制御状態(UCS)データ166などが記憶される。これにより、利用制御状態データ166がRAM領域132に記憶されることで、購入・利用形態が決定したROM型の記録媒体130となる。

メディアSAM133には、例えば、ROM型の記録媒体130の識別子であるメディアIDと、メディア鍵データK_{MED}とが記憶されている。

メディアSAM133は、例えば、相互認証機能を有している。

【0056】

また、SAM管理部124は、セキュアコンテナ104を、ネットワークやデジタル放送などを用いてオンラインでユーザホームネットワーク103に配信する場合には、暗号化・復号部121においてセッション鍵データK_{SES}を用いてセキュアコンテナ104を暗号化した後に、ネットワークを介してユーザホームネットワーク103に配信する。

本実施形態では、SAM管理部、EMDサービスセンタ管理部、並びに後述するコンテンツプロバイダ管理部およびサービスプロバイダ管理部として、例えば、内部の処理内容の監視(モニタリング)および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0057】

ここで、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給は、上述したように記録媒体130を用いて行う場合とネットワークを使ってオンラインで行う場合との何れでも権利書データ106が格納された共通の形式のセキュアコンテナ104を用いる。従って、ユーザホームネットワーク103のSAM105₁～105₄では、オフラインおよびオンラインの何れの場合でも、共通の権利書データ106に基づいた権利処理を行なうことができる。

【0058】

また、上述したように、本実施形態では、セキュアコンテナ104内に、コンテンツ鍵データK_cで暗号化されたコンテンツデータCと、当該暗号化を解くためのコンテンツ鍵データK_cとを同封するイン・バンド(In-Band)方式を採用し

ている。イン・バンド方式では、ユーザホームネットワーク103の機器で、コンテンツデータCを再生しようとするときに、コンテンツ鍵データKcを別途配信する必要がなく、ネットワーク通信の負荷を軽減できるという利点がある。また、コンテンツ鍵データKcは配信用鍵データKD₁～KD₆で暗号化されているが、配信用鍵データKD₁～KD₆は、EMDサービスセンタ102で管理されており、ユーザホームネットワーク103のSAM105₁～105₅に事前に(SAM105₁～105₄がEMDサービスセンタ102に初回にアクセスする際に)配信されているので、ユーザホームネットワーク103では、EMDサービスセンタ102との間をオンラインで接続することなく、オフラインで、コンテンツデータCの利用が可能になる。

なお、本発明は、コンテンツデータCとコンテンツ鍵データKcとを別々に、ユーザホームネットワーク103に供給するアウト・オブ・バンド(Out-Of-Band)方式を採用できる柔軟性を有している。

【0059】

EMDサービスセンタ管理部125は、EMDサービスセンタ102から6カ月分の配信用鍵データKD₁～KD₆およびそれぞれに対応した署名データSIG_{KD1,ESC}～SIG_{KD6,ESC}と、コンテンツプロバイダ101の公開鍵データK_{CP,P}を含む公開鍵証明書CER_{CP}およびその署名データSIG_{1,ESC}と、決済レポートデータ107とを受信すると、これらを暗号化・復号部121においてセッション鍵データK_{SES}を用いて復号した後に、記憶部119に記憶する。

決済レポートデータ107は、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。

【0060】

また、EMDサービスセンタ管理部125は、提供するコンテンツデータCのグローバルユニーク(Global Unique)な識別子Content_ID、公開鍵データK_{CP,P}およびそれらの署名データSIG_{g,CP}を、EMDサービスセンタ102に送信し、EMDサービスセンタ102から、公開鍵データK_{CP,P}の公開鍵証明書データCER_{CP}を入力する。

また、EMDサービスセンタ管理部125は、権利書データ106をEMDサービスセンタ102に登録する際に、図7(A)に示すように、提供するコンテンツデータCのグローバルユニークな識別子Content_ID、コンテンツ鍵データKcおよび権利書データ106を格納したモジュールMod₃と、その署名データSIG_{5,CP}とを格納した権利書登録要求用モジュールMod₂を作成し、これを暗号化・復号部121においてセッション鍵データK_{SES}を用いて暗号化した後に、ネットワークを介してEMDサービスセンタ102に送信する。

EMDサービスセンタ管理部125としては、前述したように、例えば、内部の処理内容の監視（モニタリング）および改竄ができないあるいは困難な耐タンパ性の構造を持つ通信ゲートウェイが用いられる。

【0061】

以下、図2および図3を参照しながら、コンテンツプロバイダ101における処理の流れを説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ101の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ102に登録処理を行い、グローバルユニークな識別子CP_IDを得ている。識別子CP_IDは、記憶部119に記憶される。

【0062】

以下、コンテンツプロバイダ101が、EMDサービスセンタ102に、自らの秘密鍵データK_{CP,S}に対応する公開鍵データK_{CP,S}の正当性を証明する公開鍵証明書データCER_{CP}を要求する場合の処理を図3および図8を参照しながら説明する。

図8は、当該処理のフローチャートである。

ステップSA1：コンテンツプロバイダ101は、例えば真性乱数発生器から構成される乱数発生部115を用いて乱数を発生して秘密鍵データK_{CP,S}を生成する。

ステップSA2：コンテンツプロバイダ101は、秘密鍵データK_{CP,S}に対応する公開鍵データK_{CP,P}を作成して記憶部119に記憶する。

ステップSA3：コンテンツプロバイダ101のEMDサービスセンタ管理部125は、コンテンツプロバイダ101の識別子CP_IDおよび公開鍵データ $K_{CP,P}$ を記憶部119から読み出す。

そして、EMDサービスセンタ管理部125は、識別子CP_IDおよび公開鍵データ $K_{CP,P}$ を含む公開鍵証明書データ発行要求をEMDサービスセンタ102に送信する。

ステップSA4：EMDサービスセンタ管理部125は、当該発行要求に応じて、公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ をEMDサービスセンタ102から入力して記憶部119に書き込む。

【0063】

以下、コンテンツプロバイダ101が、EMDサービスセンタ102から配信用鍵データを受信する処理を図3を参照しながら説明する。

なお、以下に示す処理を行う前提として、コンテンツプロバイダ101は、EMDサービスセンタ102から既に公開鍵証明書データ CER_{CP} を得ている必要がある。

EMDサービスセンタ管理部125が、EMDサービスセンタ102から6か月分の配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1,ESC} \sim SIG_{KD6,ESC}$ を入力し、これを記憶部119内の所定のデータベースに記憶する。

そして、署名処理部117において、記憶部119に記憶された署名データ $SIG_{KD1,ESC} \sim SIG_{KD6,ESC}$ の正当性が確認された後に、記憶部119に記憶されている配信用鍵データ $KD_1 \sim KD_6$ が有効なものとして扱われる。

【0064】

以下、コンテンツプロバイダ101がユーザホームネットワーク103のSAM105₁にセキュアコンテナ104を送信する場合の処理を図2および図9を参照しながら説明する。

図9は、当該処理のフローチャートである。

なお、以下の例では、コンテンツプロバイダ101からSAM105₁にセキュアコンテナ104を送信する場合を例示するが、セキュアコンテナ104をS

AM105₂ ~ 105₄ に送信する場合も、SAM105₁ を介して SAM105₂ ~ 105₄ に送信される点を除いて同じである。

【0065】

ステップSB1：コンテンツデータS111がコンテンツマスタソースサーバ111から読み出されて電子透かし情報付加部112に出力される。

電子透かし情報付加部112は、コンテンツデータS111に電子透かし情報を埋め込んでコンテンツデータS112を生成し、これを圧縮部113に出力する。

ステップSB2：圧縮部113は、コンテンツデータS112を、例えばATRAC3方式で圧縮してコンテンツデータS113を作成し、これを暗号化部114に出力する。

【0066】

ステップSB3：乱数発生部115は、乱数を発生してコンテンツ鍵データK_cを生成し、これを暗号化部114に出力する。

【0067】

ステップSB4：暗号化部114は、コンテンツデータS113と、記憶部119から読み出されたメタデータMetaおよびA/V伸長用ソフトウェアSoftとを、コンテンツ鍵データK_cを用いて暗号化してセキュアコンテナ作成部118に出力する。この場合に、メタデータMetaは暗号化しなくてもよい。

そして、セキュアコンテナ作成部118は、図4（A）に示すコンテンツファイルCFを作成する。また、署名処理部117において、コンテンツファイルCFのハッシュ値がとられ、秘密鍵データK_{CP,S}を用いて署名データSIG_{6,CP}が生成される。

【0068】

ステップSB5：署名処理部117は、コンテンツデータC、コンテンツ鍵データK_cおよび権利書データ106のそれぞれに対してハッシュ値をとり、秘密鍵データK_{CP,S}を用いて、それぞれのデータの作成者（提供者）の正当性を示す署名データSIG_{2,CP}、SIG_{3,CP}、SIG_{4,CP}を作成する。

また、暗号化部116は、図4（B）に示すコンテンツ鍵データK_c、権利書

データ106、SAMプログラム・ダウンロード・コンテナSD₁～SD₃ および署名・証明書モジュールMod₁を、対応する期間の配信用鍵データKD₁～KD₃で暗号化してセキュアコンテナ作成部118に出力する。

そして、セキュアコンテナ作成部118は、図4(B)に示すキーファイルKFを作成する。

また、署名処理部117は、キーファイルKFのハッシュ値をとり、秘密鍵データK_{CP,S}を用いて、署名データSIG_{7,CP}を作成する。

【0069】

ステップSB6：セキュアコンテナ作成部118は、図4(A)に示すコンテンツファイルCFおよびその署名データSIG_{6,CP}と、図4(B)に示すキーファイルKFおよびその署名データSIG_{7,CP}と、図4(C)に示す公開鍵証明書データCER_{CP}およびその署名データSIG_{1,ESC}とを格納したセキュアコンテナ104を作成し、これを、セキュアコンテナデータベース118aに記憶する。

ステップSB7：セキュアコンテナ作成部118は、例えばユーザからの要求(リクエスト)に応じてユーザホームネットワーク103に提供しようとするセキュアコンテナ104をセキュアコンテナデータベース118aから読み出して、相互認証部120とSAM105₁との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部121において暗号化した後に、SAM管理部124を介してユーザホームネットワーク103のSAM105₁に送信する。

【0070】

以下、コンテンツプロバイダ101が、EMDサービスセンタ102に権利書データ106およびコンテンツ鍵データKcを登録して権威化することを要求する場合の処理を図3を参照して説明する。

権利書データ106およびコンテンツ鍵データKcの権威化要求処理は、個々のコンテンツデータC毎に行われる。

【0071】

この場合には、署名処理部117において、記憶部119から読み出したコン

テンツデータCのグローバルユニークな識別子Content_ID、コンテンツ鍵データKcおよび権利書データ作成部122から入力した権利書データ106からなるモジュールMod₃のハッシュ値が求められ、秘密鍵データK_{CP,S}を用いて署名データSIG_{5,CP}が生成される。

そして、図7(A)に示す権利登録要求用モジュールMod₂を、相互認証部120とEMDサービスセンタ102との間の相互認証によって得られたセッション鍵データK_{SES}を用いて暗号化・復号部121において暗号化した後に、EMDサービスセンタ管理部125からEMDサービスセンタ102に送信する。

【0072】

本実施形態では、EMDサービスセンタ102において権利書データ106およびコンテンツ鍵データKcを権威化した後に、コンテンツプロバイダ101がEMDサービスセンタ102から権威化されたことを証明する権威化証明書モジュールを受信しない場合、すなわちコンテンツプロバイダ101において配信用鍵データKD₁～KD₆を用いて暗号化を行ってキーファイルKFを作成する場合を例示する。

但し、本発明は、例えば、EMDサービスセンタ102において権利書データ106およびコンテンツ鍵データKcを権威化した後に、EMDサービスセンタ102からコンテンツプロバイダ101に、配信用鍵データKD₁～KD₆を用いて暗号化した図7(B)に示す権威化証明書モジュールMod_{2a}を送信してもよい。

権威化証明書モジュールMod_{2a}は、コンテンツデータCのグローバルユニークな識別子Content_ID、コンテンツ鍵データKcおよび権利書データ作成部122から入力した権利書データ106を格納したモジュールMod_{3a}と、秘密鍵データK_{ESC,S}を用いたモジュールMod_{3a}の署名データSIG_{5a,ESC}とを格納している。

この場合には、コンテンツプロバイダ101は、例えば、セキュアコンテナ104内に、権威化証明書モジュールMod_{2a}を格納してSAM105₁～105

4に配給する。

なお、EMDサービスセンタ102は、それぞれ異なる月に対応する配信用鍵

データ $KD_1 \sim KD_6$ を用いて暗号化した6カ月分の権威化証明書モジュール Mod_{2a} を生成し、これらをまとめてコンテンツプロバイダ101に送信してもよい。

【0073】

〔EMDサービスセンタ102〕

EMDサービスセンタ102は、認証(CA:Certificate Authority)機能、鍵管理(Key Management)機能および権利処理(Rights Clearing) (利益分配)機能を有する。

図10は、EMDサービスセンタ102の機能の構成図である。

図10に示すように、EMDサービスセンタ102は、鍵サーバ141、鍵データベース141a、決算処理部142、署名処理部143、決算機関管理部144、証明書・権利書管理部145、CERデータベース145a、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150および暗号化・復号部151を有する。

なお、図10には、EMDサービスセンタ102内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ101との間で送受信されるデータに関連するデータの流れが示されている。

また、図11には、EMDサービスセンタ102内の機能ブロック相互間のデータの流れのうち、SAM105₁ ~ 105₄ および図1に示す決済機関91との間で送受信されるデータに関連するデータの流れが示されている。

【0074】

鍵サーバ141は、鍵データベース141aに記憶された各々有効期間が1カ月の配信用鍵データを要求に応じて読み出してコンテンツプロバイダ管理部148およびSAM管理部149に出力する。

また、鍵データベース141a配信用鍵データKDの他に、記録用鍵データKSTR、メディア鍵データK_{MED} およびMAC鍵データK_{MAC} などの鍵データを記憶する一連の鍵データベースからなる。

【0075】

決算処理部142は、SAM105₁～105₄から入力した利用履歴データ108と、証明書・権利書管理部145から入力した標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済レポートデータ107および決済請求権データ152を作成し、決済レポートデータ107をコンテンツプロバイダ管理部148に出力し、決済請求権データ152を決算機関管理部144に出力する。

なお、決算処理部142は、販売価格に基づいて、違法なダンピング価格による取引が行われたか否かを監視する。

ここで、利用履歴データ108は、ユーザホームネットワーク103におけるセキュアコンテナ104の購入、利用（再生、記録および転送など）の履歴を示し、決算処理部142においてセキュアコンテナ104に関連したライセンス料の支払い額を決定する際に用いられる。

【0076】

利用履歴データ108には、例えば、セキュアコンテナ104に格納されたコンテンツデータCの識別子Content_ID、セキュアコンテナ104を配給したコンテンツプロバイダ101の識別子CP_ID、セキュアコンテナ104内のコンテンツデータCの圧縮方法、セキュアコンテナ104を記録した記録媒体の識別子Media_ID、セキュアコンテナ104を配給を受けたSAM105₁～105₄の識別子SAM_ID、当該SAM105₁～105₄のユーザのUSER_IDなどが記述されている。従って、EMDサービスセンタ102は、コンテンツプロバイダ101の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク103のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータ107および決済請求権データ152を作成する。当該分配率表は、例えば、セキュアコンテナ104に格納されたコンテンツデータ毎に作成される。

また、決済請求権データ152は、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータであり、例えば、ユーザが支払った

金銭を複数の権利者に配給する場合には、個々の権利者毎に作成される。

なお、決済機関 91 は、決済が終了すると、当該決済機関の利用明細書を EMD サービスセンタ 102 に送る。EMD サービスセンタ 102 は、当該利用明細書の内容を、対応する権利者に通知する。

【0077】

決算機関管理部 144 は、決算処理部 142 が生成した決済請求権データ 152 を図 1 に示すペイメントゲートウェイ 90 を介して決済機関 91 に送信する。

なお、後述するように、決算機関管理部 144 は、決済請求権データ 152 を、コンテンツプロバイダ 101 などの権利者に送信し、権利者自らが、受信した決済請求権データ 152 を用いて決済機関 91 に決済を行ってもよい。

また、決算機関管理部 144 は、署名処理部 143 において決済請求権データ 152 のハッシュ値をとり、秘密鍵データ $K_{ESC,S}$ を用いて生成した署名データ SIG_{gg} を決済請求権データ 152 と共に決済機関 91 に送信する。

【0078】

証明書・権利書管理部 145 は、CER データベース 145a に登録されて権威化された公開鍵証明書データ CER_{CP} および公開鍵証明書データ $CER_{SAM1} \sim CER_{SAM4}$ などを読み出すと共に、コンテンツプロバイダ 101 の権利書データ 106 およびコンテンツ鍵データ K_c などを CER データベース 145a に登録して権威化する。

なお、公開鍵証明書データ $CER_{SAM1} \sim CER_{SAM4}$ を格納するデータベースと、権利書データ 106 およびコンテンツ鍵データ K_c とを個別に設けてもよい。

このとき、証明書・権利書管理部 145 は、例えば、権利書データ 106 およびコンテンツ鍵データ K_c などのハッシュ値をとり、秘密鍵データ $K_{ESC,S}$ を用いた署名データを付した権威化されたそれぞれの証明書データを作成する。

【0079】

コンテンツプロバイダ管理部 148 は、コンテンツプロバイダ 101 との間で通信する機能を有し、登録されたコンテンツプロバイダ 101 の識別子 CP_ID などを管理する CP データベース 148a にアクセスできる。

【0080】

SAM管理部149は、ユーザホームネットワーク103内のSAM105₁～105₄との間で通信する機能を有し、登録されたSAMの識別子SAM_IDやSAM登録リストなどを記録したSAMデータベース149aにアクセスできる。

【0081】

以下、EMDサービスセンタ102内での処理の流れを説明する。

まず、EMDサービスセンタ102からコンテンツプロバイダ101およびユーザホームネットワーク103内のSAM105₁～105₄への配信用鍵データを送信する際の処理の流れを、図10および図11を参照しながら説明する。

図10に示すように、鍵サーバ141は、所定期間毎に、例えば、6カ月分の配信用鍵データKD₁～KD₆を鍵データベース141aから読み出してコンテンツプロバイダ管理部148に出力する。

また、署名処理部143は、配信用鍵データKD₁～KD₆の各々のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{ESC,S}を用いて、それぞれに対応する署名データSIG_{KD1,ESC}～SIG_{KD6,ESC}を作成し、これをコンテンツプロバイダ管理部148に出力する。

コンテンツプロバイダ管理部148は、この6カ月分の配信用鍵データKD₁～KD₆およびそれらの署名データSIG_{KD1,ESC}～SIG_{KD6,ESC}を、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0082】

また、図11に示すように、鍵サーバ141は、所定期間毎に、例えば、3カ月分の配信用鍵データKD₁～KD₃を鍵データベース141aから読み出してSAM管理部149に出力する。

また、署名処理部143は、配信用鍵データKD₁～KD₃の各々のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{ESC,S}を用いて、それぞれに対応する署名データSIG_{KD1,ESC}～SIG_{KD3,ESC}を作成し、これをS

AM管理部149に出力する。

SAM管理部149は、この3カ月分の配信用鍵データ $KD_1 \sim KD_3$ およびそれらの署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ を、相互認証部150とSAM105₁ ~ 105₄ と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、SAM105₁ ~ 105₄ に送信する。

【0083】

以下、EMDサービスセンタ102がコンテンツプロバイダ101から、公開鍵証明書データ CER_{CP} の発行要求を受けた場合の処理を、図10および図12を参照しながら説明する。

図12は、当該処理のフローチャートである。

ステップSC1：コンテンツプロバイダ管理部148は、コンテンツプロバイダ101の識別子 CP_ID 、公開鍵データ $K_{CP,P}$ および署名データ $SIG_{9,CP}$ を含む公開鍵証明書データ発行要求をコンテンツプロバイダ101から受信すると、これらを、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

ステップSC2：当該復号した署名データ $SIG_{9,CP}$ の正当性を署名処理部143において確認した後に、識別子 CP_ID および公開鍵データ $K_{CP,P}$ に基づいて、当該公開鍵証明書データ発行要求を出したコンテンツプロバイダ101がCPデータベース148aに登録されているか否かを確認する。

【0084】

ステップSC3：証明書・権利書管理部145は、当該コンテンツプロバイダ101の公開鍵証明書データ CER_{CP} を CER データベース145aから読み出してコンテンツプロバイダ管理部148に出力する。

【0085】

ステップSC4：署名処理部143は、公開鍵証明書データ CER_{CP} のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データ $K_{ESC,S}$ を用いて、署名データ $SIG_{1,ESC}$ を作成し、これをコンテンツプロバイダ管理部148に出力する。

ステップSC5：コンテンツプロバイダ管理部148は、公開鍵証明書データ

CER_{CP}およびその署名データSIG_{1,ESC}を、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0086】

以下、EMDサービスセンタ102がSAM105₁から、公開鍵証明書データCER_{SAM1}の発行要求を受けた場合の処理を、図11および図13を参照しながら説明する。

図13は、当該処理のフローチャートである。

ステップSD1：SAM管理部149は、SAM105₁の識別子SAM₁ — ID、公開鍵データK_{SAM1,P}および署名データSIG_{8,SAM1}を含む公開鍵証明書データ発行要求をSAM105₁から受信すると、これらを、相互認証部150とSAM105₁と間の相互認証で得られたセッション鍵データK_{SES}を用いて復号する。

【0087】

ステップSD2：当該復号した署名データSIG_{8,SAM1}の正当性を署名処理部143において確認した後に、識別子SAM₁ — IDおよび公開鍵データK_{SAM1,P}に基づいて、当該公開鍵証明書データの発行要求を出したSAM105₁がSAMデータベース149aに登録されているか否かを確認する。

ステップSD3：証明書・権利書管理部145は、当該SAM105₁の公開鍵証明書データCER_{SAM1}をCERデータベース145aから読み出してSAM管理部149に出力する。

【0088】

ステップSD4：署名処理部143は、公開鍵証明書データCER_{SAM1}のハッシュ値をとり、EMDサービスセンタ102の秘密鍵データK_{ESC,S}を用いて、署名データSIG_{50,ESC}を作成し、これをSAM管理部149に出力する。

ステップSD5：SAM管理部149は、公開鍵証明書データCER_{SAM1}およびその署名データSIG_{50,ESC}を、相互認証部150とSAM105₁と間の相互認証で得られたセッション鍵データK_{SES}を用いて暗号化した後に、SAM105₁に送信する。

なお、 $SAM105_2 \sim 105_4$ が、公開鍵証明書データを要求した場合の処理は、対象が $SAM105_2 \sim 105_4$ に代わるのみで、基本的に上述した $SAM105_1$ の場合と同じである。

なお、本発明では、EMDサービスセンタ102は、例えば、 $SAM105_1$ の出荷時に、 $SAM105_1$ の秘密鍵データ $K_{SAM1,S}$ および公開鍵データ $K_{SAM1,P}$ を $SAM105_1$ の記憶部に記憶する場合には、当該出荷時に、公開鍵データ $K_{SAM1,P}$ の公開鍵証明書データ CER_{SAM1} を作成してもよい。

このとき、当該出荷時に、公開鍵証明書データ CER_{SAM1} を、 $SAM105_1$ の記憶部に記憶してもよい。

【0089】

以下、EMDサービスセンタ102が、コンテンツプロバイダ101から権利書データ106およびコンテンツ鍵データ K_c の登録要求を受けた場合の処理を、図10および図14を参照しながら説明する。

図14は、当該処理のフローチャートである。

ステップSE1：コンテンツプロバイダ管理部148は、コンテンツプロバイダ101から図7(A)に示す権利書登録要求モジュール Mod_2 を受信すると、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データ K_{SES} を用いて権利書登録要求モジュール Mod_2 を復号する。

【0090】

ステップSE2：署名処理部143において、鍵データベース141aから読み出した公開鍵データ K_{cp} を用いて、署名データ $SIG_{5,CP}$ の正当性を検証する。

ステップSE3：証明書・権利書管理部145は、権利書登録要求モジュール Mod_2 に格納された権利書データ106およびコンテンツ鍵データ K_c を、 CER データベース145aに登録する。

【0091】

以下、EMDサービスセンタ102において決済処理を行なう場合の処理を図11および図15を参照しながら説明する。

図15は、当該処理のフローチャートである。

ステップSF1：SAM管理部149は、ユーザホームネットワーク103の例えばSAM105₁から利用履歴データ108およびその署名データSIG_{200,SAM1}を入力すると、利用履歴データ108および署名データSIG_{200,SAM1}を、相互認証部150とSAM105₁との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、SAM105₁の公開鍵データK_{SAM1}による署名データSIG_{200,SAM1}の検証を行なった後に、決算処理部142に出力する。

【0092】

ステップSF2：決算処理部142は、SAM管理部149から入力した利用履歴データ108と、証明書・権利書管理部145を介してCERデータベース145aから読み出した権利書データ106に含まれる標準小売価格データSRPおよび販売価格とに基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を生成する。なお、決済請求権データ152および決済レポートデータ107の生成は、SAMから利用履歴データ108を入力する度に行ってもよいし、所定の期間毎に行ってもよい。

ステップSF3：決算処理部142は、決済請求権データ152を決算機関管理部144に出力する。

決算機関管理部144は、決済請求権データ152およびその署名データSIG₉₉を、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図1に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152に示される金額の金銭が、コンテンツプロバイダ101に支払われる。

なお、EMDサービスセンタ102は、決済請求権データ152をコンテンツプロバイダ101に送信し、コンテンツプロバイダ101が決済請求権データ152を用いて決済記載91に金銭を請求してもよい。

【0093】

ステップSF4：決算処理部142は、決済レポートデータ107をコンテンツプロバイダ管理部148に出力する。

決済レポートデータ107は、上述したように、例えば、EMDサービスセンタ102が図1に示す決済機関91に対して行なったコンテンツプロバイダ101に関する決済の内容が記述されている。

コンテンツプロバイダ管理部148は、決済レポートデータ107を、相互認証部150と図3に示す相互認証部120と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、コンテンツプロバイダ101に送信する。

【0094】

また、EMDサービスセンタ102は、前述したように、権利書データ106を登録（権威化）した後に、EMDサービスセンタ102からコンテンツプロバイダ101に、図7（B）に示す権威化証明書モジュール Mod_{2a} を配信用鍵データ $KD_1 \sim KD_6$ で暗号化して送信してもよい。

【0095】

また、EMDサービスセンタ102は、その他に、 $SAM105_1 \sim 105_4$ の出荷時の処理と、SAM登録リストの登録処理とを行なうが、これらの処理については後述する。

【0096】

〔ユーザホームネットワーク103〕

ユーザホームネットワーク103は、図1に示すように、ネットワーク機器160₁ およびA/V機器160₂ ~ 160₄ を有している。

ネットワーク機器160₁ は、 $SAM105_1$ を内蔵している。また、AV機器160₂ ~ 160₄ は、それぞれ $SAM105_2 \sim 105_4$ を内蔵している。

$SAM105_1 \sim 105_4$ の相互間は、例えば、IEEE1394シリアルインタフェースバスなどのバス191を介して接続されている。

なお、AV機器160₂ ~ 160₄ は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器160₁ のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク103は、ネットワーク機能を有していない

AV機器のみを有していてもよい。

【0097】

以下、ネットワーク機器160₁について説明する。

図16ネットワーク機器160₁の構成図である。

図16に示すように、ネットワーク機器160₁は、SAM105₁、通信モジュール162、復号・伸長モジュール163、購入・利用形態決定操作部165、ダウンロードメモリ167、再生モジュール169および外部メモリ201を有する。

【0098】

SAM105₁～105₄は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ102との間で通信を行う。

SAM105₁～105₄は、例えば、EMDサービスセンタ102によって仕様およびバージョンなどが管理され、家庭機器メーカーに対し、搭載の希望があればコンテンツ単位の課金を行うブラックボックスの課金モジュールとしてライセンス譲渡される。例えば、家庭機器開発メーカーは、SAM105₁～105₄のIC(Integrated Circuit)の内部の仕様を知ることとはできず、EMDサービスセンタ102が当該ICのインタフェースなどを統一化し、それに従ってネットワーク機器160₁およびAV機器160₂～160₄に搭載される。

【0099】

SAM105₁～105₄は、その処理内容が外部から完全に遮蔽され、その処理内容を外部から監視および改竄不能であり、また、内部に予め記憶されているデータおよび処理中のデータを外部から監視および改竄不能な耐タンパ(Tamper Resistance)性を持ったハードウェアモジュール(ICモジュールなど)である。

SAM105₁～105₄の機能をICという形で実現する場合は、IC内部に秘密メモリを持ち、そこに秘密プログラムおよび秘密データが格納される。SAMをICという物理的形態にとらわれず、その機能を機器の何れかの部分に組み込むことができれば、その部分をSAMとして定義してもよい。

【0100】

以下、SAM105₁の機能について詳細に説明する。

なお、SAM105₂～105₄は、SAM105₁と基本的に同じ機能を有している。

図17は、SAM105₁の機能の構成図である。

なお、図17には、コンテンツプロバイダ101からのセキュアコンテナ104を入力し、セキュアコンテナ104内のキーファイルKFを復号する処理に関連するデータの流れが示されている。

図17に示すように、SAM105₁は、相互認証部170、暗号化・復号部171、172、173、コンテンツプロバイダ管理部180、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、課金処理部187、署名処理部189、SAM管理部190、メディアSAM管理部197、スタック（作業）メモリ200および外部メモリ管理部811を有する。

なお、AV機器160₂～160₄はダウンロードメモリ167を有していないため、SAM105₂～105₄にはダウンロードメモリ管理部182は存在しない。

【0101】

なお、図17に示すSAM105₁の所定の機能は、例えば、図示しないCPUにおいて秘密プログラムを実行することによって実現される。

また、スタックメモリ200には、以下に示す処理を経て、図18に示すように、利用履歴データ108およびSAM登録リストが記憶される。

ここで、外部メモリ201のメモリ空間は、SAM105₁の外部（例えば、ホストCPU810）からは見ることはできず、SAM105₁のみが外部メモリ201の記憶領域に対してのアクセスを管理できる。

外部メモリ201としては、例えば、フラッシュメモリあるいは強誘電体メモリ（FeRAM）などが用いられる。

また、スタックメモリ200としては、例えばSARAMが用いられ、図19

に示すように、セキュアコンテナ104、コンテンツ鍵データ K_c 、権利書データ(UCP)106、記憶部192のロック鍵データ K_{LOC} 、コンテンツプロバイダ101の公開鍵証明書 CER_{CP} 、利用制御状態データ(UCS)166、およびSAMプログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ などが記憶される。

【0102】

以下、 $SAM105_1$ の機能のうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力したときの各機能ブロックの処理内容を図17を参照しながら説明する。

【0103】

相互認証部170は、 $SAM105_1$ がコンテンツプロバイダ101およびEMDサービスセンタ102との間でオンラインでデータを送受信する際に、コンテンツプロバイダ101およびEMDサービスセンタ102との間で相互認証を行ってセッション鍵データ(共有鍵) K_{SES} を生成し、これを暗号化・復号部171に出力する。セッション鍵データ K_{SES} は、相互認証を行う度に新たに生成される。

【0104】

暗号化・復号部171は、コンテンツプロバイダ101およびEMDサービスセンタ102との間で送受信するデータを、相互認証部170が生成したセッション鍵データ K_{SES} を用いて暗号化・復号する。

【0105】

誤り訂正部181は、セキュアコンテナ104を誤り訂正してダウンロードメモリ管理部182に出力する。

なお、ユーザホームネットワーク103は、セキュアコンテナ104が改竄されているか否かを検出する機能を有していてもよい。

本実施形態では、誤り訂正部181を、 $SAM105_1$ に内蔵した場合を例示したが、誤り訂正部181の機能を、例えばホストCPU810などの $SAM105_1$ の外部に持たせてもよい。

【0106】

ダウンロードメモリ管理部182は、図16に示すようにダウンロードメモリ167が相互認証機能を持つメディアSAM167aを有している場合には、相互認証部170とメディアSAM167aとの間で相互認証を行った後に、誤り訂正後のセキュアコンテナ104を、相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化して図16に示すダウンロードメモリ167に書き込む。ダウンロードメモリ167としては、例えば、メモリスティックなどの不揮発性半導体メモリが用いられる。

なお、図20に示すように、HDD(Hard Disk Drive)などの相互認証機能を備えていないメモリをダウンロードメモリ211として用いる場合には、ダウンロードメモリ211内はセキュアではないので、コンテンツファイルCFをダウンロードメモリ211にダウンロードし、機密性の高いキーファイルKFを例えば、図17に示すスタックメモリ200にダウンロードする。

【0107】

セキュアコンテナ復号部183は、ダウンロードメモリ管理部182から入力したセキュアコンテナ104に格納されたキーファイルKFを、記憶部192から読み出した対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて復号し、署名処理部189において署名データ $SIG_{2,CP} \sim SIG_{4,CP}$ の正当性、すなわちコンテンツデータC、コンテンツ鍵データ K_c および権利書データ106の作成者の正当性を確認した後に、スタックメモリ200に書き込む。

【0108】

EMDサービスセンタ管理部185は、図1に示すEMDサービスセンタ102との間の通信を管理する。

【0109】

署名処理部189は、記憶部192から読み出したEMDサービスセンタ102の公開鍵データ $K_{ESC,P}$ およびコンテンツプロバイダ101の公開鍵データ $K_{CP,P}$ を用いて、セキュアコンテナ104内の署名データの検証を行なう。

【0110】

記憶部192は、SAM105₁の外部から読み出しおよび書き換えできない

秘密データとして、図21に示すように、配信用鍵データ $KD_1 \sim KD_3$ 、SAM_ID、ユーザID、パスワード、情報参照用ID、SAM登録リスト、記録用鍵データ K_{STR} 、ルートCAの公開鍵データ $K_{R-CA,P}$ 、EMDサービスセンタ102の公開鍵データ $K_{ESC,P}$ 、メディア鍵データ K_{MED} 、EMDサービスセンタ102の公開鍵データ $K_{ESC,P}$ 、SAM105₁の秘密鍵データ $K_{SAM1,S}$ 、SAM105₁の公開鍵データ $K_{SAM1,P}$ を格納した公開鍵証明書 CER_{SAM1} 、EMDサービスセンタ102の秘密鍵データ $K_{ESC,S}$ を用いた公開鍵証明書 CER_{ESC} の署名データ SIG_{22} 、復号・伸長モジュール163との間の相互認証用の元鍵データ、メディアSAMとの間の相互認証用の元鍵データを記憶している。

また、記憶部192には、図17に示す少なくとも一部の機能を実現するための秘密プログラムが記憶されている。

記憶部192としては、例えば、フラッシューEEPROM(Electrically Erasable Programmable RAM)が用いられる。

【0111】

以下、SAM105₁の処理の流れのうち、コンテンツプロバイダ101からのセキュアコンテナ104を入力したときの処理の流れを説明する。

まず、EMDサービスセンタ102から受信した配信用鍵データ $KD_1 \sim KD_3$ を記憶部192に格納する際のSAM105₁内での処理の流れを図17を参照しながら説明する。

この場合には、まず、相互認証部170と図10に示す相互認証部150との間で相互認証が行われる。

次に、当該相互認証によって得られたセッション鍵データ K_{SES} で暗号化された3カ月分の配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ が、EMDサービスセンタ102からEMDサービスセンタ管理部185を介してスタックメモリ811に書き込まれる。

次に、暗号化・復号部171において、セッション鍵データ K_{SES} を用いて、配信用鍵データ $KD_1 \sim KD_3$ およびその署名データ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ が復号される。

次に、署名処理部189において、スタックメモリ811に記憶された署名デ

ータ $SIG_{KD1,ESC} \sim SIG_{KD3,ESC}$ の正当性が確認された後に、配信用鍵データ $KD_1 \sim KD_3$ が記憶部 192 に書き込まれる。

【0112】

以下、セキュアコンテナ 104 をコンテンツプロバイダ 101 から入力し、セキュアコンテナ 104 内のキーファイル KF を復号する際の $SAM105_1$ 内での処理の流れを図 17 および図 22 を参照しながら説明する。

図 22 は、当該処理のフローチャートである。

ステップ SG1：図 17 に示す $SAM105_1$ の相互認証部 170 と図 2 に示す相互認証部 120 との間で相互認証が行なわれる。

暗号化・復号部 171 は、当該相互認証によって得られたセッション鍵データ K_{SES} を用いて、コンテンツプロバイダ管理部 180 を介してコンテンツプロバイダ 101 から受信したセキュアコンテナ 104 を復号する。

【0113】

ステップ SG2：署名処理部 189 は、図 4 (C) に示す署名データ SIG_1, ESC の検証を行なった後に、図 4 (C) に示す公開鍵証明書データ CER_{CP} 内に格納されたコンテンツプロバイダ 101 の公開鍵データ $K_{CP,P}$ を用いて、署名データ $SIG_{6,CP}, SIG_{7,CP}$ の正当性を確認する。

コンテンツプロバイダ管理部 180 は、署名データ $SIG_{6,CP}, SIG_{7,CP}$ の正当性が確認されると、セキュアコンテナ 104 を誤り訂正部 181 に出力する。

誤り訂正部 181 は、セキュアコンテナ 104 を誤り訂正した後に、ダウンロードメモリ管理部 182 に出力する。

【0114】

ステップ SG3：ダウンロードメモリ管理部 182 は、相互認証部 170 と図 16 に示すメディア $SAM167a$ との間で相互認証を行なった後に、セキュアコンテナ 104 をダウンロードメモリ 167 に書き込む。

【0115】

ステップ SG4：ダウンロードメモリ管理部 182 は、相互認証部 170 と図 16 に示すメディア $SAM167a$ との間で相互認証を行なった後に、セキュア

コンテナ104に格納された図4（B）に示すキーファイルKFをダウンロードメモリ167から読み出してセキュアコンテナ復号部183に出力する。

そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて、キーファイルKFを復号し、図4（B）に示す署名・証明書モジュール Mod_1 に格納された署名データ $SIG_{1,ESC}$ 、 $SIG_{2,CP} \sim SIG_{4,CP}$ を署名処理部189に出力する。

【0116】

ステップSG5：署名処理部189は、図4（B）に示す署名データ $SIG_{1,ESC}$ の検証を行なった後に、図4（B）に示す公開鍵証明書データ CER_{CP} 内に格納された公開鍵データ $K_{ESC,P}$ を用いて署名データ $SIG_{2,CP} \sim SIG_{4,CP}$ の検証を行なう。これにより、コンテンツデータC、コンテンツ鍵データ K_c および権利書データ106の作成者の正当性が検証される。

【0117】

ステップSG6：セキュアコンテナ復号部183は、署名データ $SIG_{2,CP} \sim SIG_{4,CP}$ の正当性が確認されると、キーファイルKFをスタックメモリ200に書き込む。

【0118】

以下、ダウンロードメモリ167にダウンロードされたコンテンツデータCを利用・購入する処理に関連する各機能ブロックの処理内容を図23を参照しながら説明する。

【0119】

利用監視部186は、スタックメモリ200から権利書データ106および利用制御状態データ166を読み出し、当該読み出した権利書データ106および利用制御状態データ166によって許諾された範囲内でコンテンツの購入・利用が行われるように監視する。

ここで、権利書データ106は、図17を用いて説明したように、復号後にスタックメモリ200に記憶された図4（B）に示すキーファイルKF内に格納されている。

また、利用制御状態データ166は、後述するように、ユーザによって購入形

態が決定されたときに、スタックメモリ200に記憶される。

【0120】

課金処理部187は、図16に示す購入・利用形態決定操作部165からの操作信号S165に応じた利用履歴データ108を作成する。

ここで、利用履歴データ108は、前述したように、ユーザによるセキュアコンテナ104の購入および利用の形態の履歴を記述しており、EMDサービスセンタ102において、セキュアコンテナ104の購入に応じた決済処理およびラインセンス料の支払いを決定する際に用いられる。

【0121】

また、課金処理部187は、必要に応じて、スタックメモリ200から読み出した販売価格あるいは標準小売価格データSRPをユーザに通知する。

ここで、販売価格および標準小売価格データSRPは、復号後にスタックメモリ200に記憶された図4(B)に示すキーファイルKFの権利書データ106内に格納されている。

課金処理部187による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御状態データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行う。

【0122】

また、課金処理部187は、操作信号S165に基づいて、ユーザによるコンテンツの購入形態を記述した利用制御状態(UCS: Usage Control Status)データ166を生成し、これをスタックメモリ200に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ166には、コンテンツのID、購入形態、当該購入形態に応じた価

格、当該コンテンツの購入が行なわれたSAMのSAM_ID、購入を行なったユーザのUSER_IDなどが記述されている。

【0123】

なお、決定された購入形態が再生課金である場合には、例えば、SAM105₁からコンテンツプロバイダ101に利用制御状態データ166をコンテンツデータCの購入と同時にリアルタイムに送信し、コンテンツプロバイダ101がEMDサービスセンタ102に、利用履歴データ108を所定の期間内にSAM105₁に取りにいくことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ166が、コンテンツプロバイダ101およびEMDサービスセンタ102の双方にリアルタイムに送信される。このように、本実施形態では、何れの場合にも、利用制御状態データ166をコンテンツプロバイダ101にリアルタイムに送信する。

【0124】

EMDサービスセンタ管理部185は、外部メモリ管理部811を介して外部メモリ201から読み出した利用履歴データ108をEMDサービスセンタ102に送信する。

このとき、EMDサービスセンタ管理部185は、署名処理部189において、秘密鍵データ $K_{SAM1,s}$ を用いて利用履歴データ108の署名データ $SIG_{200,SAM1}$ を作成し、署名データ $SIG_{200,SAM1}$ を利用履歴データ108と共にEMDサービスセンタ102に送信する。

EMDサービスセンタ102への利用履歴データ108の送信は、例えば、EMDサービスセンタ102からの要求に応じてあるいは定期的に行ってもよいし、利用履歴データ108に含まれる履歴情報の情報量が所定以上になったときに行ってもよい。当該情報量は、例えば、外部メモリ201の記憶容量に応じて決定される。

【0125】

ダウンロードメモリ管理部182は、例えば、図16に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの再生動作が行われる場合

に、ダウンロードメモリ167から読み出したコンテンツデータC、スタックメモリ200から読み出したコンテンツ鍵データKcおよび課金処理部187から入力したユーザ電子透かし情報用データ196を復号・伸長モジュール管理部184に出力する。

また、復号・伸長モジュール管理部184は、図16に示す購入形態決定操作部165からの操作信号S165に応じてコンテンツの試聴動作が行われる場合に、ダウンロードメモリ167から読み出したコンテンツファイルCF、並びにスタックメモリ200から読み出したコンテンツ鍵データKcおよび半開示パラメータデータ199を復号・伸長モジュール管理部184に出力する。

【0126】

ここで、半開示パラメータデータ199は、権利書データ106内に記述されており、試聴モード時のコンテンツの取り扱いを示している。復号・伸長モジュール163では、半開示パラメータデータ199に基づいて、暗号化されたコンテンツデータCを、半開示状態で再生することが可能になる。半開示の手法としては、例えば、復号・伸長モジュール163がデータ（信号）を所定のブロックを単位として処理することを利用して、半開示パラメータデータ199によって、コンテンツ鍵データKcを用いて復号を行うブロックと復号を行わないブロックとを指定したり、試聴時の再生機能を限定したり、試聴可能な期間を限定するものなどがある。

【0127】

以下、SAM105₁ 内での処理の流れについて説明する。

まず、コンテンツプロバイダ101からダウンロードメモリ167にダウンロードされたセキュアコンテナ104の購入形態を決定するまでの処理の流れを図23および図24を参照しながら説明する。

図24は、当該処理のフローチャートである。

ステップSH1：課金処理部187において、ユーザによる図16に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が発生したか否かが判断され、発生したと判断された場合にはステップSH2の処理が行われ、そうでない場合にはステップSH3の処理が行われる。

【0128】

ステップSH2：課金処理部187によって、例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図16に示す復号・伸長モジュール163に出力される。

このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データ K_{SES} による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データ K_{SES} による暗号化・復号とが行なわれる。

コンテンツファイルCFは、図16に示す復号部221において復号された後に、復号部222に出力される。

【0129】

また、スタックメモリ200から読み出されたコンテンツ鍵データ K_c および半開示パラメータデータ199が、図16に示す復号・伸長モジュール163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データ K_c および半開示パラメータデータ199に対してセッション鍵データ K_{SES} による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ199が半開示処理部225に出力され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データ K_c を用いたコンテンツデータCの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長された後に、電子透かし情報処理部224に出力される。

次に、電子透かし情報処理部224においてユーザ電子透かし情報用データ196がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される。

【0130】

ステップSH3：ユーザが購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。

ステップSH4：課金処理部187において、決定された購入形態に応じた利

用履歴データ108および利用制御状態データ166が生成され、利用履歴データ108が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に、利用制御状態データ166がスタックメモリ200に書き込まれる。

以後は、利用監視部186において、利用制御状態データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

【0131】

ステップSH5：スタックメモリ200に格納されているキーファイルKFに、利用制御状態データ166が加えられ、購入形態が決定した後述する図29（B）に示す新たなキーファイルKF₁が生成される。キーファイルKF₁は、スタックメモリ200に記憶される。

図29（B）に示すように、キーファイルKF₁に格納された利用制御状態データ166はストレージ鍵データK_{STR}を用いてDESのCBCモードを利用して暗号化されている。また、当該ストレージ鍵データK_{STR}をMAC鍵データとして用いて生成したMAC値であるMAC₃₀₀が付されている。また、利用制御状態データ166およびMAC₃₀₀からなるモジュールは、メディア鍵データK_{MED}を用いてDESのCBCモードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データK_{MED}をMAC鍵データとして用いて生成したMAC値であるMAC₃₀₁が付されている。

【0132】

以下、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図23および図25を参照しながら説明する。

図25は、当該処理のフローチャートである。

ステップSI1：課金処理部187が、ユーザによる操作に応じて、再生を行うコンテンツを指定した操作信号S165を入力する。

ステップSI2：課金処理部187は、利用監視部186の監視下で、操作信号S165に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが読み出される。

【0133】

ステップS I 3 : 当該読み出されたコンテンツファイルCFが図16に示す復号・伸長モジュール163に出力される。このとき、図23に示す相互認証部170と、図16に示す復号・伸長モジュール163の相互認証部220との間で相互認証が行われる。

また、スタックメモリ200から読み出されたコンテンツ鍵データKcが復号・伸長モジュール163に出力される。

【0134】

ステップS I 4 : 復号・伸長モジュール163の復号部222において、コンテンツ鍵データKcを用いたコンテンツファイルCFの復号と、伸長部223による伸長処理とが行なわれ、再生モジュール169において、コンテンツデータCが再生される。

ステップS I 5 : 課金処理部187によって、操作信号S165に応じて、外部メモリ201に記憶されている利用履歴データ108が更新される。

利用履歴データ108は、外部メモリ201から読み出された後、相互認証を経て、EMDサービスセンタ管理部185を介して、署名データSIG_{200,SAM1}と共にEMDサービスセンタ102に送信される。

【0135】

以下、図26に示すように、例えば、ネットワーク機器160₁のダウンロードメモリ167にダウンロードされた既に購入形態が決定されたコンテンツファイルCFおよびキーファイルKFを、バス191を介して、AV機器160₂のSAM105₂に転送する場合のSAM105₁内での処理の流れを図27および図28を参照しながら説明する。

図28は、当該処理のフローチャートである。

ステップS J 1 : ユーザは、購入・利用形態決定操作部165を操作して、ダウンロードメモリ167に記憶された所定のコンテンツをAV機器160₂に転送することを指示し、当該操作に応じた操作信号S165が、課金処理部187に出力される。

これにより、課金処理部187は、操作信号S165に基づいて、外部メモリ

201に記憶されている利用履歴データ108を更新する。

【0136】

ステップSJ2：ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図29（A）に示すコンテンツファイルCFをSAM管理部190に出力する。

ステップSJ3：スタックメモリ200から読み出した図29（B）に示すキーファイルKF₁を、署名処理部189およびSAM管理部190に出力する。

ステップSJ4：署名処理部189は、スタックメモリ200から読み出したキーファイルKF₁の署名データSIG_{42,SAM1}を作成し、これをSAM管理部190に出力する。

また、SAM管理部190は、記憶部192から、図29（C）に示す公開鍵証明書データCER_{SAM1}およびその署名データSIG_{22,ESC}を読み出す。

【0137】

ステップSJ5：相互認証部170は、SAM105₂との間で相互認証を行って得たセッション鍵データK_{SES}を暗号化・復号部171に出力する。

SAM管理部190は、図29（A），（B），（C）に示すデータからなる新たなセキュアコンテナを作成する。

ステップSJ6：暗号化・復号部171において、セッション鍵データK_{SES}を用いて暗号化した後に、図26に示すAV機器160₂のSAM105₂に出力する。

このとき、SAM105₁とSAM105₂との間の相互認証と並行して、IEEE1394シリアルバスであるバス191の相互認証が行われる。

【0138】

以下、図26に示すように、SAM105₁から入力したコンテンツファイルCFなどを、RAM型などの記録媒体（メディア）に書き込む際のSAM105₂内での処理の流れを、図30および図31を参照しながら説明する。

図31は、当該処理のフローチャートである。

【0139】

ステップSK1：SAM105₂のSAM管理部190は、図26に示すよう

に、図29 (A) に示すコンテンツファイルCFと、図29 (B) に示すキーファイルKF₁ およびその署名データSIG_{42,SAM1} と、図29 (C) に示す公開鍵署名データCER_{SAM1} およびその署名データSIG_{22,ESC}とを、ネットワーク機器160₁ のSAM105₁ から入力する。

そして、暗号化・復号部171において、SAM管理部190が入力したコンテンツファイルCFと、キーファイルKF₁ およびその署名データSIG_{42,SAM1} と、公開鍵署名データCER_{SAM1} およびその署名データSIG_{22,ESC}とが、相互認証部170とSAM105₁ の相互認証部170との間の相互認証によって得られたセッション鍵データK_{SES} を用いて復号される。

次に、セッション鍵データK_{SES} を用いて復号されたキーファイルKF₁ およびその署名データSIG_{42,SAM1} と、公開鍵署名データCER_{SAM1} およびその署名データSIG_{22,ESC}とが、スタックメモリ200に書き込まれる。

【0140】

ステップSK2：署名処理部189は、スタックメモリ200から読み出した署名データSIG_{22,ESC}を、記憶部192から読み出した公開鍵データK_{ESC,P}を用いて検証して、公開鍵証明書データCER_{SAM1}の正当性を確認する。

そして、署名処理部189は、公開鍵証明書データCER_{SAM1}の正当性を確認すると、公開鍵証明書データCER_{SAM1}に格納された公開鍵データK_{SAM1,P}を用いて、署名データSIG_{42,SAM1}の正当を確認する。

次に、署名データSIG_{42,SAM1}の正当性、すなわちキーファイルKF₁の作成者の正当性が確認されると、図29 (B) に示すキーファイルKF₁をスタックメモリ200から読み出して暗号化・復号部173に出力する。

なお、当該例では、キーファイルKF₁の作成者と送信元とが同じ場合を述べたが、キーファイルKF₁の作成者と送信元とが異なる場合には、キーファイルKF₁に対して作成者の署名データと送信者と署名データとが作成され、署名処理部189において、双方の署名データの正当性が検証される。

【0141】

ステップSK3：暗号化・復号部173は、記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED} および購入者鍵データK_{PIN}を用い

てキーファイル K_{F1} を順に暗号化してメディアSAM管理部197に出力する。

なお、メディア鍵データ K_{MED} は、図27に示す相互認証部170と図26に示すRAM型の記録媒体250のメディアSAM252との間の相互認証によって記憶部192に事前に記憶されている。

【0142】

ここで、記録用鍵データ K_{STR} は、例えばSACD(Super Audio Compact Disc)、DVD(Digital Versatile Disc)機器、CD-R機器およびMD(Mini Disc)機器などの種類(当該例では、AV機器160₂)に応じて決まるデータであり、機器の種類と記録媒体の種類とを1対1で対応づけるために用いられる。なお、SACDとDVDとでは、ディスク媒体の物理的な構造が同じであるため、DVD機器を用いてSACDの記録媒体の記録・再生を行うことができる場合がある。記録用鍵データ K_{STR} は、このような場合において、不正コピーを防止する役割を果たす。

【0143】

また、メディア鍵データ K_{MED} は、記録媒体(当該例では、RAM型の記録媒体250)にユニークなデータである。

メディア鍵データ K_{MED} は、記録媒体(当該例では、図26に示すRAM型の記録媒体250)側に格納されており、記録媒体のメディアSAMにおいてメディア鍵データ K_{MED} を用いた暗号化および復号を行うことがセキュリティの観点から好ましい。このとき、メディア鍵データ K_{MED} は、記録媒体にメディアSAMが搭載されている場合には、当該メディアSAM内に記憶されており、記録媒体にメディアSAMが搭載されていない場合には、例えば、RAM領域内のホストCPU810の管理外の領域に記憶されている。

なお、本実施形態のように、機器側のSAM(当該例では、SAM105₂)とメディアSAM(当該例では、メディアSAM252)との間で相互認証を行い、セキュアな通信経路を介してメディア鍵データ K_{MED} を機器側のSAMに転送し、機器側のSAMにおいてメディア鍵データ K_{MED} を用いた暗号化および復号を行なってもよい。

本実施形態では、記録用鍵データ K_{STR} およびメディア鍵データ K_{MED} が、記録媒体の物理層のレベルのセキュリティを保護するために用いられる。

【0144】

また、購入者鍵データ K_{PIN} は、コンテンツファイルCFの購入者を示すデータであり、例えば、コンテンツを買い切りで購入したときに、当該購入したユーザに対してEMDサービスセンタ102によって割り当てられる。購入者鍵データ K_{PIN} は、EMDサービスセンタ102において管理される。

【0145】

ステップSK4：メディアSAM管理部197は、SAM管理部190から入力したコンテンツファイルCFおよび暗号化・復号部173から入力したキーファイル KF_1 を、図26に示す記録モジュール260に出力する。

そして、記録モジュール260は、メディアSAM管理部197から入力したコンテンツファイルCFおよびキーファイル KF_1 を、図26に示すRAM型の記録媒体250のRAM領域251に書き込む。この場合に、キーファイル KF_1 を、メディアSAM252内に書き込むようにしてもよい。

【0146】

以下、コンテンツの購入形態が未決定の図6に示すROM型の記録媒体130をユーザホームネットワーク303がオフラインで配給を受けた場合に、AV機器160₂ において購入形態を決定する際の処理の流れを図32、図33、図34、図35を参照しながら説明する。

ステップSL1：AV機器160₂ のSAM105₂ は、先ず、図33に示す相互認証部170と図6に示すROM型の記録媒体130のメディアSAM133との間で相互認証を行った後に、メディアSAM133からメディア鍵データ K_{MED} を入力する。

なお、SAM105₂ が、事前にメディア鍵データ K_{MED} を保持している場合には、当該入力を行わなくても良い。

【0147】

ステップSL2：ROM型の記録媒体130のRAM領域132に記録されているセキュアコンテナ104に格納された図4(B)，(C)に示すキーファイ

ルKFおよびその署名データ $SIG_{7,CP}$ と、公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ とが、メディアSAM管理部197を介して入力され、これらがスタックメモリ200に書き込まれる。

【0148】

ステップSL3：署名処理部189において、署名データ $SIG_{1,ESC}$ の正当性を確認した後に、公開鍵証明書データ CER_{CP} から公開鍵データ $K_{CP,P}$ を取り出し、この公開鍵データ $K_{CP,P}$ を用いて、署名データ $SIG_{7,CP}$ の正当性、すなわちキーファイルKFの作成者の正当性を検証する。

【0149】

ステップSL4：署名処理部189において署名データ $SIG_{7,CP}$ の正当性が確認されると、スタックメモリ200からセキュアコンテナ復号部183に、キーファイルKFを読み出す。

そして、セキュアコンテナ復号部183において、対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて、キーファイルKFを復号する。

【0150】

ステップSL5：署名処理部189において、公開鍵データ $K_{ESC,P}$ を用いて、キーファイルKFに格納された署名データ $SIG_{1,ESCM}$ の正当性を確認した後に、キーファイルKF内の公開鍵証明書データ CER_{CP} に格納された公開鍵データ $K_{CP,P}$ を用いて、署名データ $SIG_{2,CP} \sim SIG_{4,CP}$ の正当性、すなわちコンテンツデータC、コンテンツ鍵データKcおよび権利書データ106の作成者の正当性を検証する。

【0151】

ステップSL6：課金処理部187において、ユーザによる図16に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が発生したか否かが判断され、発生したと判断された場合にはステップSL7の処理が行われ、そうでない場合にはステップSL8の処理が行われる。

【0152】

ステップSL7：図33に示す相互認証部170と図32に示す復号・伸長モジュール163との間で相互認証を行った後に、 $SAM105_2$ の復号・伸長モ

ジュール管理部 184 は、スタックメモリ 200 に記憶されているコンテンツ鍵データ K_c および権利書データ 106 に格納された半開示パラメータデータ 199、並びに ROM 型の記録媒体 130 の ROM 領域 131 から読み出したコンテンツデータ C を図 32 に示す復号・伸長モジュール 163 に出力する。次に、復号・伸長モジュール 163 において、コンテンツデータ C がコンテンツ鍵データ K_c を用いて半開示モードで復号された後に伸長され、再生モジュール 270 に出力される。そして、再生モジュール 270 において、復号・伸長モジュール 163 からのコンテンツデータ C が試聴モードで再生される。

【0153】

ステップ SL8 : ユーザによる図 32 に示す購入形態決定操作部 165 の購入操作によってコンテンツの購入形態が決定され、当該決定された購入形態を示す操作信号 S165 が課金処理部 187 に入力される。

【0154】

ステップ SL9 : 課金処理部 187 は、操作信号 S165 に応じた利用制御状態データ 166 を作成し、これをスタックメモリ 200 に書き込む。

また、課金処理部 187 は、利用履歴データ 108 を作成あるいは更新する。

【0155】

ステップ SL10 : スタックメモリ 200 から暗号化・復号部 173 に、例えば、図 4 (B) に示すキーファイル K_F に利用制御状態データ 166 を格納した図 29 (B) に示す新たなキーファイル K_{F1} が出力される。

【0156】

ステップ SL11 : 暗号化・復号部 173 は、スタックメモリ 200 から読み出した図 29 (B) に示すキーファイル K_{F1} を、記憶部 192 から読み出した記録用鍵データ K_{STR}、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を用いて順次に暗号化してメディア SAM 管理部 197 に出力する。

【0157】

ステップ SL12 : 図 33 に示す相互認証部 170 と図 32 に示すメディア SAM 133 との間で相互認証を行った後に、SAM 管理部 197 は、暗号化・復号部 173 から入力したキーファイル K_{F1} を図 32 に示す記録モジュール 27

1 を介して ROM 型の記録媒体 130 の RAM 領域 132 あるいはメディア SAM133 内に書き込む。

これにより、購入形態が決定された ROM 型の記録媒体 130 が得られる。

このとき、課金処理部 187 が生成した利用制御状態データ 166 および利用履歴データ 108 は、所定のタイミングで、スタックメモリ 200 および外部メモリ 201 からそれぞれ読み出しされた EMD サービスセンタ 102 に送信される。

【0158】

以下、図 36 に示すように、AV 機器 160₃ において購入形態が未決定の ROM 型の記録媒体 130 からセキュアコンテナ 104 を読み出して AV 機器 160₂ に転送し、AV 機器 160₂ において購入形態を決定して RAM 型の記録媒体 250 に書き込む際の処理の流れを図 37 および図 38 を用いて説明する。

図 37 は、SAM105₃ における当該処理のフローチャートである。

図 38 は、SAM105₂ における当該処理のフローチャートである。なお、ROM 型の記録媒体 130 から RAM 型の記録媒体 250 へのセキュアコンテナ 104 の転送は、図 1 に示すネットワーク機器 160₁ および AV 機器 160₁ ~ 160₄ のいずれの間で行ってもよい。

【0159】

ステップ SM11 (図 37) : AV 機器 160₃ の SAM105₃ と ROM 型の記録媒体 130 のメディア SAM133 との間で相互認証を行い、ROM 型の記録媒体 130 のメディア鍵データ K_{MED1} を SAM105₃ に転送する。

このとき、同様に、V 機器 160₂ の SAM105₂ と RAM 型の記録媒体 250 のメディア SAM252 との間で相互認証を行い、RAM 型の記録媒体 250 のメディア鍵データ K_{MED2} を SAM105₂ に転送する。

【0160】

ステップ SM12 : SAM105₃ は、RAM 領域 132 から読み出した図 4 (B), (C) キーファイル KF、署名データ $SIG_{7,CP}$ 、公開鍵証明書データ CER_{CP} およびその署名データ $SIG_{1,ESC}$ とを、図 40 に示す暗号化・復号部 172 において、対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて順に復

号する。

次に、暗号化・復号部172で復号されたコンテンツファイルCFは、暗号化・復号部171に出力され、 $SAM105_3$ と 105_2 との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化された後に、SAM管理部190に出力される。

また、暗号化・復号部172で復号されたキーファイルKFは、暗号化・復号部171および署名処理部189に出力される。

【0161】

ステップSM13：署名処理部189は、 $SAM105_3$ の秘密鍵データ $K_{SAM3,S}$ を用いて、キーファイルKFの署名データ $SIG_{350,SAM3}$ を作成し、これを暗号化・復号部171に出力する。

【0162】

ステップSM14：暗号化・復号部171は、記憶部192から読み出した $SAM105_3$ の公開鍵証明書データ CER_{SAM3} およびその署名データ $SIG_{351,ESC}$ と、キーファイルKFおよびその署名データ $SIG_{350,SAM3}$ と、ROM型の記録媒体130のROM領域131から読み出した図4(A)に示すコンテンツファイルCFとを、 $SAM105_3$ と 105_2 との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化した後に、SAM管理部190を介して、AV機器160₂ の $SAM105_2$ に出力する。

【0163】

ステップSN1（図38）： $SAM105_2$ では、図41に示すように、SAM管理部190を介して $SAM105_3$ から入力されたコンテンツファイルCFが、暗号化・復号部171においてセッション鍵データ K_{SES} を用いて復号された後に、メディアSAM管理部197を介してRAM型の記録媒体250のRAM領域251に書き込まれる。

また、SAM管理部190を介して $SAM105_3$ から入力されたキーファイルKFおよびその署名データ $SIG_{350,SAM3}$ と、公開鍵証明書データ CER_{SAM3} およびその署名データ $SIG_{351,ESC}$ とが、スタックメモリ200に書き込まれた後に、暗号化・復号部171においてセッション鍵データ K_{SES} を用いて復号

される。

【0164】

ステップSN2：当該復号された署名データSIG_{351,ECS}が、署名処理部189において署名検証され、その正当性が確認されると、公開鍵証明書データCER_{SAM3}に格納された公開鍵データK_{SAM3}を用いて、署名データSIG_{350,SAM3}の正当性、すなわちキーファイルKFの送信元の正当性が確認される。

そして、署名データSIG_{350,SAM3}の正当性が確認されると、スタックメモリ200からキーファイルKFが読み出されてセキュアコンテナ復号部183に出力される。

【0165】

ステップSN3：セキュアコンテナ復号部183は、対応する期間の配信用鍵データKD₁～KD₃を用いて、キーファイルKFを復号し、所定の署名検証を経た後に、当該復号したキーファイルKFをスタックメモリ200に書き込む。

その後、スタックメモリ200に記憶されている既に復号されたキーファイルKFに格納された権利書データ106が、利用監視部186に出力される。そして、利用監視部186によって、権利書データ106に基づいて、コンテンツの購入形態および利用形態が管理される。

【0166】

ステップSN4：課金処理部187において、ユーザによる図16に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が発生したか否かが判断され、発生したと判断された場合にはステップSN5の処理が行われ、そうでない場合にはステップSN6の処理が行われる。

【0167】

ステップSN5：ユーザによって試聴モードが選択されると、既にセッション鍵データK_{SES}で復号されたコンテンツファイルCFのコンテンツデータCと、スタックメモリ200に記憶されたコンテンツ鍵データK_c、権利書データ106から得られた半開示パラメータデータ199およびユーザ電子透かし情報用データ196とが、相互認証を経た後に、図36に示す復号・伸長モジュール管理部184を介して再生モジュール270に出力される。そして、再生モジュール

270において、試聴モードに対応したコンテンツデータCの再生が行われる。

【0168】

ステップSN6：ユーザによる図36に示す購入・利用形態決定操作部165の操作によってコンテンツの購入・利用形態が決定され、当該決定に応じた操作信号S165が、課金処理部187に出力される。

ステップSN7：課金処理部187において、決定された購入・利用形態に応じて利用制御状態データ166および利用履歴データ108が生成され、これがスタックメモリ200および外部メモリ201にそれぞれ書き込まれる。

【0169】

ステップSN8：スタックメモリ200から読み出された利用制御状態データ166を格納した例えば図29(B)に示すキーファイルKF₁が作成され、これが暗号化・復号部173に出力される。

ステップSN9：暗号化・復号部173において記憶部192から読み出した記録用鍵データK_{STR}、メディア鍵データK_{MED2}および購入者鍵データK_{PIN}を用いて順に暗号化され、メディアSAM管理部197に出力される。

ステップSN10：メディアSAM管理部197によって、キーファイルKF₁が、図36に示す記録モジュール271によってRAM型の記録媒体250のRAM領域251あるいはメディアSAM252に書き込まれる。

また、利用制御状態データ166および利用履歴データ108は、所定のタイミングで、EMDサービスセンタ102に送信される。

以下、SAM105₁～105₄の実現方法について説明する。

SAM105₁～105₄の機能をハードウェアとして実現する場合は、メモリを内蔵したASIC型のCPUを用いて、そのメモリには、図17に示す各機能を実現するためのセキュリティー機能モジュールやコンテンツの権利処理をおこなうプログラムモジュールおよび鍵データなどの機密性の高いデータが格納される。暗号ライブラリーモジュール（公開鍵暗号、共通鍵暗号、乱数発生器、ハッシュ関数）、コンテンツの使用制御用のプログラムモジュール、課金処理のプログラムモジュールなど、一連の権利処理用のプログラムモジュールは、例えば、ソフトウェアとして実装される。

【0170】

例えば、図17に示す暗号化・復号部171などのモジュールは、例えば、処理速度の問題でハードウェアとしてASIC型のCPU内のIPコアとして実装される。クロック速度やCPUコード体系などの性能によっては、暗号化・復号部171をソフトウェアとして実装してもよい。

また、図17に示す記憶部192や、図17に示す機能を実現するためのプログラムモジュールおよびデータを格納するメモリとしては、例えば、不揮発メモリ（フラッシュROM）が用いられ、作業用メモリとしてはSRAMなどの高速書き込み可能なメモリが用いられる。なお、その他にも、SAM105₁～105₄に内蔵されるメモリとして、強誘電体メモリ（FeRAM）を用いてもよい。

また、SAM105₁～105₄には、その他に、コンテンツの利用のための有効期限や契約期間などで日時の検証に使用する時計機能が内蔵されている。

【0171】

上述したように、SAM105₁～105₄は、プログラムモジュールや、データおよび処理内容を外部から遮蔽した耐タンパ性の構造を持っている。SAM105₁～105₄を搭載した機器のホストCPUのバス経由で、当該SAMのIC内部のメモリに格納されている秘密性の高いプログラムおよびデータの内容や、SAMのシステムコンフィギュレーション(System Configuration)関連のレジスタ群および暗号ライブラリーや時計のレジスタ群などの値が、読み出されたり、新規に書き込まれたりしないように、すなわち、搭載機器のホストCPUが割り付けているアドレス空間内に存在しないように、当該SAMでは、CPU側のメモリー空間を管理するMMU(Memory Magagement Unit)を用いて、搭載機器側のホストCPUからは見えないアドレス空間を設定する。

また、SAM105₁～105₄は、X線や熱などの外部からの物理的な攻撃にも耐え得る構造をもち、さらにデバッグ用ツール（ハードウェアICE、ソフトウェアICE）などを用いたリアルタイムデバッグ（リバースエンジニアリング）が行われても、その処理内容が分からないか、あるいは、デバッグ用ツールそのものがIC製造後には使用できないような構造をしている。

SAM105₁ ~ 105₄ 自身は、ハードウェア的な構造においては、メモリを内蔵した通常のASIC型のCPUであり、機能は当該CPUを動作させるソフトウェアに依存するが、暗号機能と耐タンパ性のハードウェア構造を有している点が、一般的なASIC型のCPUと異なる。

【0172】

SAM105₁ ~ 105₄ の機能を全てソフトウェアで実現する場合は、耐タンパ性を持ったモジュール内部で閉じてソフトウェア処理をおこなう場合と、通常のセットに搭載されているホストCPU上のソフトウェア処理で行い、当該処理のときにのみ解読することが不可能となる仕掛けをする場合とがある。前者は、暗号ライブラリモジュールがIPコアではなく、通常のソフトウェアモジュールとしてメモリに格納される場合と同じであり、ハードウェアとして実現する場合と同様に考えられる。一方、後者は、タンパーレジスタントソフトウェアと呼ばれるもので、ICE（デバッガ）で実行状況を解読されても、そのタスクの実行順序がバラバラであったり（この場合には、区切ったタスク単体でプログラムとしての意味があるように、すなわち前後のラインに影響がでないようにタスク切りを行う）、タスクそのものが暗号化されており、一種のセキュア処理を目的としたタスクスケジューラ（MiniOS）と同様に実現できる。当該タスクスケジューラは、ターゲットプログラムに埋め込まれている。

【0173】

次に、図16に示す復号・伸長モジュール163について説明する。

図16に示すように、復号・伸長モジュール163は、相互認証部220、復号部221、復号部222、伸長部223、電子透かし情報処理部224および半開示処理部225を有する。

相互認証部220は、復号・伸長モジュール163がSAM105₁ からデータを入力する際に、図26に示す相互認証部170との間で相互認証を行ってセッション鍵データK_{SES} を生成する。

【0174】

復号部221は、SAM105₁ から入力したコンテンツ鍵データK_c、半開示パラメータデータ199、ユーザ電子透かし情報用データ196およびコンテ

ンツデータCを、セッション鍵データ K_{SES} を用いて復号する。そして、復号部221は、復号したコンテンツ鍵データ K_c およびコンテンツデータCを復号部222に出力し、復号したユーザ電子透かし情報用データ196を電子透かし情報処理部224に出力し、半開示パラメータデータ199を半開示処理部225に出力する。

【0175】

復号部222は、半開示処理部225からの制御に基づいて、コンテンツ鍵データ K_c を用いて、コンテンツデータCを半開示状態で復号し、復号したコンテンツデータCを伸長部223に出力する。

【0176】

伸長部223は、復号されたコンテンツデータCを伸長して、電子透かし情報処理部224に出力する。

伸長部223は、例えば、図4(A)に示すコンテンツファイルCFに格納されたA/V伸長用ソフトウェアを用いて伸長処理を行い、例えば、ATRAC3方式で伸長処理を行う。

【0177】

電子透かし情報処理部224は、復号されたユーザ電子透かし情報用データ196に応じたユーザ電子透かし情報を、復号されたコンテンツデータCに埋め込み、新たなコンテンツデータCを生成する。電子透かし情報処理部224は、当該新たなコンテンツデータCを再生モジュール169に出力する。

このように、ユーザ電子透かし情報は、コンテンツデータCを再生するとき、復号・伸長モジュール163において埋め込まれる。

なお、本発明では、コンテンツデータCにユーザ電子透かし情報用データ196を埋め込まないようにしてもよい。

【0178】

半開示処理部225は、半開示パラメータデータ199に基づいて、例えば、コンテンツデータCのうち復号を行わないブロックと、復号を行うブロックとを復号部222に指示する。

また、半開示処理部225は、その他に、半開示パラメータデータ199に基

づいて、試聴時の再生機能を限定したり、試聴可能な期間を限定するなどの制御を行う。

【0179】

再生モジュール169は、復号および伸長されたコンテンツデータCに応じた再生を行う。

【0180】

次に、コンテンツプロバイダ101、EMDサービスセンタ102およびユーザホームネットワーク103の間で、秘密鍵データを用いて生成した署名データを付したデータおよび公開鍵証明書データを送受信する際のデータフォーマットについて説明する。

図42(A)は、コンテンツプロバイダ101からSAM105₁にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からSAM105₁に、コンテンツプロバイダ101とSAM105₁との間の相互認証によって得たセッション鍵データK_{SES}で暗号化したモジュールMod₅₀が送信される。

モジュールMod₅₀には、モジュールMod₅₁およびその秘密鍵データK_{CP,S}による署名データSIG_{CP}が格納されている。

モジュールMod₅₁には、コンテンツプロバイダ101の秘密鍵データK_{CP,P}を格納した公開鍵証明書データCER_{CP}と、公開鍵証明書データCER_{CP}対しての秘密鍵データK_{ESC,S}による署名データSIG_{ESC}と、送信するデータDataとが格納されている。

このように、公開鍵証明書データCER_{CP}を格納したモジュールMod₅₀を、コンテンツプロバイダ101からSAM105₁に送信することで、SAM105₁において署名データSIG_{CP}の検証を行なう際に、EMDサービスセンタ102からSAM105₁に公開鍵証明書データCER_{CP}を送信する必要がなくなる。

【0181】

図42(B), (C)は、コンテンツプロバイダ101からSAM105₁に

データ $Data$ をアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ 101 から $SAM105_1$ に、コンテンツプロバイダ 101 と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図 4 2 (B) に示すモジュール Mod_{52} が送信される。

モジュール Mod_{52} には、送信するデータ $Data$ と、その秘密鍵データ $K_{CP,S}$ による署名データ SIG_{CP} とが格納されている。

また、EMDサービスセンタ 102 から $SAM105_1$ には、EMDサービスセンタ 102 と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図 4 2 (C) に示すモジュール Mod_{53} が送信される。

モジュール Mod_{53} には、コンテンツプロバイダ 101 の公開鍵証明書データ CER_{CP} と、その秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} とが格納されている。

【0182】

図 4 2 (D) は、 $SAM105_1$ からコンテンツプロバイダ 101 にデータ $Data$ をイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、 $SAM105_1$ からコンテンツプロバイダ 101 に、コンテンツプロバイダ 101 と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化したモジュール Mod_{54} が送信される。

モジュール Mod_{54} には、モジュール Mod_{55} およびその秘密鍵データ $K_{SAM1,S}$ による署名データ SIG_{SAM1} が格納されている。

モジュール Mod_{55} には、 $SAM105_1$ の秘密鍵データ $K_{SAM1,P}$ を格納した公開鍵証明書データ CER_{SAM1} と、公開鍵証明書データ CER_{SAM1} に対しての秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} と、送信するデータ $Data$ とが格納されている。

このように、公開鍵証明書データ CER_{SAM1} を格納したモジュール Mod_{55} を、 $SAM105_1$ からコンテンツプロバイダ 101 に送信することで、コンテ

ツプロバイダ101において署名データ SIG_{SAM1} の検証を行なう際に、EMDサービスセンタ102からコンテンツプロバイダ101に公開鍵証明書データ CER_{SAM1} を送信する必要がなくなる。

【0183】

図42(E), (F)は、 $SAM105_1$ からコンテンツプロバイダ101にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、 $SAM105_1$ からコンテンツプロバイダ101に、コンテンツプロバイダ101と $SAM105_1$ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図42(E)に示すモジュール Mod_{56} が送信される。

モジュール Mod_{56} には、送信するデータDataと、その秘密鍵データ $K_{SAM1,S}$ による署名データ SIG_{SAM1} とが格納されている。

また、EMDサービスセンタ102からコンテンツプロバイダ101には、EMDサービスセンタ102とコンテンツプロバイダ101との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図42(F)に示すモジュール Mod_{57} が送信される。

モジュール Mod_{57} には、 $SAM105_1$ の公開鍵証明書データ CER_{SAM1} と、その秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} とが格納されている。

【0184】

図43(G)は、コンテンツプロバイダ101からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化したモジュール Mod_{58} が送信される。

モジュール Mod_{58} には、モジュール Mod_{59} およびその秘密鍵データ $K_{CP,S}$ による署名データ SIG_{CP} が格納されている。

モジュールMod₅₉には、コンテンツプロバイダ101の秘密鍵データ $K_{CP,P}$ を格納した公開鍵証明書データ CER_{CP} と、公開鍵証明書データ CER_{CP} に対しての秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} と、送信するデータDataとが格納されている。

【0185】

図43 (H) は、コンテンツプロバイダ101からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、コンテンツプロバイダ101からEMDサービスセンタ102に、コンテンツプロバイダ101とEMDサービスセンタ102との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化した図43 (H) に示すモジュールMod₆₀が送信される。

モジュールMod₆₀には、送信するデータDataと、その秘密鍵データ $K_{CP,S}$ による署名データ SIG_{CP} とが格納されている。

このとき、EMDサービスセンタ102にはコンテンツプロバイダ101の公開鍵証明書データ CER_{CP} は既に登録されている。

【0186】

図43 (I) は、SAM105₁ からEMDサービスセンタ102にデータDataをイン・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁ からEMDサービスセンタ102に、EMDサービスセンタ102とSAM105₁ との間の相互認証によって得たセッション鍵データ K_{SES} で暗号化したモジュールMod₆₁が送信される。

モジュールMod₆₁には、モジュールMod₆₂およびその秘密鍵データ $K_{SAM1,S}$ による署名データ SIG_{SAM1} が格納されている。

モジュールMod₆₂には、SAM105₁ の秘密鍵データ $K_{SAM1,P}$ を格納した公開鍵証明書データ CER_{SAM1} と、公開鍵証明書データ CER_{SAM1} に対しての秘密鍵データ $K_{ESC,S}$ による署名データ SIG_{ESC} と、送信するデータDataとが格納されている。

【0187】

図43 (J) は、SAM105₁ からEMDサービスセンタ102にデータDataをアウト・オブ・バンド方式で送信する場合のデータフォーマットを説明するための図である。

この場合には、SAM105₁ からEMDサービスセンタ102に、EMDサービスセンタ102とSAM105₁ との間の相互認証によって得たセッション鍵データK_{SES} で暗号化した図43 (J) に示すモジュールMod₆₃が送信される。

モジュールMod₆₃には、送信するデータDataと、その秘密鍵データK_{SAM1,S}による署名データSIG_{SAM1}とが格納されている。

このとき、EMDサービスセンタ102にはSAM105₁ の公開鍵証明書データCER_{SAM1}は既に登録されている。

【0188】

以下、SAM105₁ ~ 105₄ の出荷時におけるEMDサービスセンタ102への登録処理について説明する。

なお、SAM105₁ ~ 105₄ の登録処理は同じであるため、以下、SAM105₁ の登録処理について述べる。

SAM105₁ の出荷時には、図11に示すEMDサービスセンタ102の鍵サーバ141によって、SAM管理部149を介して、図17などに示す記憶部192に以下に示す鍵データが初期登録される。

また、SAM105₁ には、例えば、出荷時に、記憶部192などに、SAM105₁ がEMDサービスセンタ102に初回にアクセスする際に用いられるプログラムなどが記憶される。

すなわち、記憶部192には、例えば、図21において左側に「*」が付されているSAM105₁ の識別子SAM_ID、記録用鍵データK_{STR}、ルート認証局2の公開鍵データK_{R-CA}、EMDサービスセンタ102の公開鍵データK_{ESC,P}、SAM105₁ の秘密鍵データK_{SAM1,S}、公開鍵証明書データCER_{SAM1}およびその署名データSIG_{22,ESC}、復号・伸長モジュール163およびメディアSAMとの間の認証用鍵データを生成するための元鍵データが初期登録で記憶

される。

なお、公開鍵証明書データ CER_{SAM1} は、 $SAM105_1$ を出荷後に登録する際に EMD サービスセンタ 102 から $SAM105_1$ に送信してもよい。

【0189】

ここで、ルート認証局 2 の公開鍵データ K_{R-CA} は、インターネットの電子商取引などでは一般的に使用されている RSA を使用し、データ長は例えば 1024 ビットである。公開鍵データ K_{R-CA} は、図 1 に示すルート認証局 2 によって発行される。

また、EMD サービスセンタ 102 の公開鍵データ $K_{ESC,P}$ は、短いデータ長で RSA と同等あるいはそれ以上の強度を持つ楕円曲線暗号を利用して生成され、データ長は例えば 160 ビットである。但し、暗号化の強度を考慮すると、公開鍵データ $K_{ESC,P}$ は 192 ビット以上であることが望ましい。また、EMD サービスセンタ 102 は、ルート認証局 92 に公開鍵データ $K_{ESC,P}$ を登録する。

また、ルート認証局 92 は、公開鍵データ $K_{ESC,P}$ の公開鍵証明書データ CER_{ESC} を作成する。公開鍵データ $K_{ESC,P}$ を格納した公開鍵証明書データ CER_{ESC} は、好ましく、 $SAM105_1$ の出荷時に記憶部 192 に記憶される。この場合に、公開鍵証明書データ CER_{ESC} は、ルート認証局 92 の秘密鍵データ $K_{ROOT,S}$ で署名されている。

【0190】

EMD サービスセンタ 102 は、乱数を発生して $SAM105_1$ の秘密鍵データ $K_{SAM1,S}$ を生成し、これとペアとなる公開鍵データ $K_{SAM1,P}$ を生成する。

また、EMD サービスセンタ 102 は、ルート認証局 92 の認証をもらって、公開鍵データ $K_{SAM1,P}$ の公開鍵証明書データ CER_{SAM1} を発行し、これに自らの秘密鍵データ $K_{ESC,S}$ を用いて署名データを添付する。すなわち、EMD サービスセンタ 102 は、セカンド CA（認証局）として機能を果たす。

【0191】

また、 $SAM105_1$ には、図 11 に示す EMD サービスセンタ 102 の SAM 管理部 149 により、EMD サービスセンタ 102 の管理下にある一意（ユニーク）な識別子 SAM_ID が割り当てられ、これが $SAM105_1$ の記憶部 1

92に格納されると共に、図11に示すSAMデータベース149aにも格納され、EMDサービスセンタ102によって管理される。

【0192】

また、SAM105₁は、出荷後、例えば、ユーザによってEMDサービスセンタ102と接続され、登録手続を行うと共に、EMDサービスセンタ102から記憶部192に配信用鍵データKD₁～KD₃が転送される。

すなわち、SAM105₁を利用するユーザは、コンテンツをダウンロードする前にEMDサービスセンタ102に登録手続が必要である。この登録手続は、例えば、SAM105₁を搭載している機器（当該例では、ネットワーク機器160₁）を購入したときに添付された登録用紙などを用いて、ユーザ本人が自己を特定する情報を記載して例えば郵便などのオフラインで行なわれる。

SAM105₁は、上述した登録手続を経た後でないと使用できない。

【0193】

EMDサービスセンタ102は、SAM105₁のユーザによる登録手続に応じて、ユーザに固有の識別子USER_IDを発行し、例えば、図11に示すSAMデータベース149aにおいて、SAM_IDとUSER_IDとの対応関係を管理し、課金時に利用する。

また、EMDサービスセンタ102は、SAM105₁のユーザに対して情報参照用識別子IDと、初回に使用されるパスワードを割り当て、これをユーザに通知する。ユーザは、情報参照用識別子IDとパスワードとを用いて、EMDサービスセンタ102に、例えば現在までのコンテンツデータの利用状況（利用履歴）などを情報の問い合わせを行なうことができる。

また、EMDサービスセンタ102は、ユーザの登録時に、クレジットカード会社などに身分の確認を行なったり、オフラインで本人の確認を行なう。

【0194】

次に、図21に示すように、SAM105₁内の記憶部192にSAM登録リストを格納する手順について説明する。

図1に示すSAM105₁は、例えば、バス191としてIEEE1394シリアルバスを用いた場合に、バス191に接続された機器の電源を立ち上げたり

、新しい機器をバス191に接続したときに生成されるトポロジーマップを利用して、自分の系に存在するSAM105₂ ~ SAM105₄のSAM登録リストを得る。

なお、IEEE1394シリアルバスであるバス191に応じて生成されたトポロジーマップは、例えば、図44に示すように、バス191にSAM105₁ ~ 105₄に加えてAV機器160₅、160₆のSCMS処理回路105₅、105₆が接続されている場合に、SAM105₁ ~ 105₄およびSCMS処理回路105₅、105₆を対象として生成される。

従って、SAM105₁は、当該トポロジーマップから、SAM105₁ ~ 105₄についての情報を抽出してSAM登録リストを生成する。

【0195】

SAM登録リストのデータフォーマットは、例えば、図45に示される。

そして、SAM105₁は、当該SAM登録リストを、EMDサービスセンタ102に登録して署名を得る。

これらの処理は、バス191のセッションを利用してSAM105₁が自動的に、EMDサービスセンタ102にSAM登録リストの登録命令を発行する。

EMDサービスセンタ102は、SAM105₁から図45に示すSAM登録リストを受けると、有効期限を確認する。そして、EMDサービスセンタ102は、登録時にSAM105₁より指定された決済機能の有無を参照して対応する部分の設定を行う。また、EMDサービスセンタ102は、リボケーションリストをチェックしてSAM登録リスト内のリボケーションフラグを設定する。リボケーションリストは、例えば、不正使用などを理由にEMDサービスセンタ102によって使用が禁止されている（無効な）SAMのリストである。

また、EMDサービスセンタ102は、決済時にはSAM105₁に対応するSAM登録リストを取り出し、その中に記述されたSAMがリボケーションリストに含まれているかを確認する。また、EMDサービスセンタ102は、SAM登録リストに署名を添付する。

なお、SAMリボケーションリストは、同一系の（同一のバス191に接続さ

れている) SAMのみを対象として生成され、各SAMに対応するリボケーションフラグによって、当該SAMの有効および無効を示している。

【0196】

以下、図1に示すコンテンツプロバイダ101の全体動作について説明する。

図46は、コンテンツプロバイダ101の全体動作のフローチャートである。

ステップS1: EMDサービスセンタ102は、コンテンツプロバイダ101が所定の登録処理を経た後に、コンテンツプロバイダ101の公開鍵データ K_{CP} , P の公開鍵証明書 CER_{CP} をコンテンツプロバイダ101に送信する。

また、EMDサービスセンタ102は、SAM105₁~105₄が所定の登録処理を経た後に、SAM105₁~105₄の公開鍵データ $K_{SAM1,P}$ ~ $K_{SAM4,P}$ の公開鍵証明書 CER_{CP1} ~ CER_{CP4} をSAM105₁~105₄に送信する。

また、EMDサービスセンタ102は、相互認証を行った後に、各々有効期限が1カ月の6カ月分の配信用鍵データ KD_1 ~ KD_6 をコンテンツプロバイダ101に送信し、3カ月分の配信用鍵データ KD_1 ~ KD_3 をユーザホームネットワーク103に送信する。

このように、EMDシステム100では、配信用鍵データ KD_1 ~ KD_3 を予めSAM105₁~105₄に配給しているため、SAM105₁~105₄とEMDサービスセンタ102との間がオフラインの状態でも、SAM105₁~105₄においてコンテンツプロバイダ101から配給されたセキュアコンテンツ104を復号して購入・利用できる。この場合に、当該購入・利用の履歴は利用履歴データ108に記述され、利用履歴データ108は、SAM105₁~105₄とEMDサービスセンタ102とが接続されたときに、EMDサービスセンタ102に自動的に送信されるため、EMDサービスセンタ102における決済処理を確実に行うことができる。なお、EMDサービスセンタ102が、所定の期間内に、利用履歴データ108を回収できないSAMについては、リボケーションリストで無効の対象とする。

なお、利用制御状態データ166は、原則として、リアルタイムで、SAM105₁~105₄からEMDサービスセンタ102に送信される。

【0197】

ステップS2：コンテンツプロバイダ101は、相互認証を行った後に、図7(A)に示す権利登録要求モジュールMod₂を、EMDサービスセンタ102に送信する。

そして、EMDサービスセンタ102は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データKcを登録して権威化する。

【0198】

ステップS3：コンテンツプロバイダ101は、対応する期間の配信用鍵データKD₁～KD₆などを用いて暗号化を行って、図4(A)，(B)に示すコンテンツファイルCFおよびキーファイルKFを作成し、これらと図4(C)に示す公開鍵証明書データCER_{cp}とを格納したセキュアコンテナ104を、オンラインおよび／またはオフラインで、ユーザホームネットワーク103に配給する。

【0199】

ステップS4：ユーザホームネットワーク103のSAM105₁～SAM105₄は、セキュアコンテナ104を対応する期間の配信用鍵データKD₁～KD₃などを用いて復号し、セキュアコンテナ104の作成者および送信者と正当性を検証するための署名検証などを行い、セキュアコンテナ104が正当なコンテンツプロバイダ101から送信されたか否かを確認する。

【0200】

ステップS5：SAM105₁～SAM105₄において、ユーザによる図16に示す購入・利用形態決定操作部165の操作に応じた操作信号S165に基づいて、購入・利用形態を決定する。

このとき、図23に示す利用監視部186において、セキュアコンテナ104に格納された権利書データ106に基づいて、ユーザによるコンテンツファイルCFの購入・利用形態が管理される。

【0201】

ステップS6：SAM105₁～SAM105₄の図23に示す課金処理部187において、操作信号S165に基づいて、ユーザによる購入・利用形態の決

定の操作を記述した利用履歴データ108および利用制御状態データ166が生成し、これらをEMDサービスセンタ102に送信する。

【0202】

ステップS7: EMDサービスセンタ102は、図11に示す決算処理部142において、利用履歴データ108に基づいて決済処理を行い、決済請求権データ152および決済レポートデータ107を作成する。EMDサービスセンタ102は、決済請求権データ152およびその署名データSIG₉₉を、図1に示すペイメントゲートウェイ90を介して、決済機関91に送信する。また、EMDサービスセンタ102は、決済レポートデータ107をコンテンツプロバイダ101に送信する。

【0203】

ステップS8: 決済機関91において、署名データSIG₉₉の検証を行った後に、決済請求権データ152に基づいて、ユーザが支払った金額が、コンテンツプロバイダ101の所有者に分配される。

【0204】

以上説明したように、EMDシステム100では、図4に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ101からユーザホームネットワーク103に配給し、セキュアコンテナ104内のキーファイルKFについての処理をSAM105₁~105₄内で行う。

また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD₁~KD₃を用いて暗号化されており、配信鍵データKD₁~KD₃を保持しているSAM105₁~105₄内でのみ復号される。そして、SAM105₁~105₄では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

従って、EMDシステム100によれば、ユーザホームネットワーク103におけるコンテンツデータCの購入および利用を、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。

【0205】

また、EMDシステム100では、コンテンツプロバイダ101からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオフラインの何れの場合でもセキュアコンテナ104を用いて行うことで、SAM105₁～105₄におけるコンテンツデータCの権利処理を双方の場合において共通化できる。

【0206】

また、EMDシステム100では、ユーザホームネットワーク103内のネットワーク機器160₁ およびAV機器160₂～160₄ においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【0207】

第1実施形態の第1変形例

上述した実施形態では、図4（B）に示すように、コンテンツプロバイダ101において配信用鍵データKDを用いてキーファイルKFを暗号化し、SAM105₁～105₄ において配信用鍵データKDを用いてキーファイルKFを復号する場合を例示したが、図1に示すように、コンテンツプロバイダ101からSAM105₁～105₄ にセキュアコンテナ104を直接供給する場合には、配信用鍵データKDを用いたキーファイルKFの暗号化は必ずしも行なわなくてもよい。このように、配信用鍵データKDを用いてキーファイルKFを暗号化することは、後述する第2実施形態のように、コンテンツプロバイダからユーザホームネットワークにサービスプロバイダを介してコンテンツデータを供給する場合に、配信用鍵データKDをコンテンツプロバイダおよびユーザホームネットワークにのみ保持させることで、サービスプロバイダによる不正行為を抑制する際に大きな効果を発揮する。

但し、上述した第1実施形態の場合でも、配信用鍵データKDを用いてキーファイルKFを暗号化することは、コンテンツデータの不正利用の抑制力を高める点で効果がある。

【0208】

また、上述した実施形態では、図4（B）に示すキーファイルKF内の権利書データ106内に標準小売価格データSRPを格納する場合を例示したが、セキュアコンテナ104内のキーファイルKFの外に、標準小売価格データSRP（プライスタグデータ）を格納してもよい。この場合には、標準小売価格データSRPに対して秘密鍵データ K_{cp} を用いて作成した署名データを添付する。

【0209】

第1実施形態の第2変形例

上述した第1実施形態では、図1に示すように、EMDサービスセンタ102が、自らが生成した決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91で決済処理を行なう場合を例示したが、例えば、図47に示すように、EMDサービスセンタ102からコンテンツプロバイダ101に決済請求権データ152を送信し、コンテンツプロバイダ101自らが、決済請求権データ152を用いて、ペイメントゲートウェイ90を介して決済機関91に対して決済処理を行なってもよい。

【0210】

第1実施形態の第3変形例

上述した第1実施形態では、単数のコンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁～105₄に、セキュアコンテナ104を供給する場合を例示したが、2以上のコンテンツプロバイダ101a、101bからSAM105₁～105₄にそれぞれセキュアコンテナ104a、104bを供給するようにしてもよい。

図48は、コンテンツプロバイダ101a、101bを用いる場合の第1実施形態の第3変形例に係わるEMDシステムの構成図である。

この場合には、EMDサービスセンタ102は、コンテンツプロバイダ101aおよび101bに、それぞれ6カ月分の配信用鍵データ $KDa_1 \sim KDa_6$ および $KDb_1 \sim KDb_6$ を配信する。

また、EMDサービスセンタ102は、SAM105₁～105₄に、3カ月分の配信用鍵データ $KDa_1 \sim KDa_3$ および $KDb_1 \sim KDb_3$ を配信する。

【0211】

そして、コンテンツプロバイダ101aは、独自のコンテンツ鍵データKcaを用いて暗号化したコンテンツファイルCfaと、コンテンツ鍵データKcaおよび権利書データ106aなどを対応する期間の配信用鍵データKDa₁～KDa₆を用いて暗号化したキーファイルKfaとを格納したセキュアコンテナ104aをSAM105₁～105₄にオンラインおよび／またはオフランで供給する。

このとき、キーファイルの識別子として、EMDサービスセンタ102が配付するグローバルユニークな識別子Content_IDが用いられ、EMDサービスセンタ102によって、コンテンツデータが一元的に管理される。

また、コンテンツプロバイダ101bは、独自のコンテンツ鍵データKcbを用いて暗号化したコンテンツファイルCfbと、コンテンツ鍵データKcbおよび権利書データ106bなどを対応する期間の配信用鍵データKDb₁～KDb₆を用いて暗号化したキーファイルKfbとを格納したセキュアコンテナ104bをSAM105₁～105₄にオンラインおよび／またはオフランで供給する。

【0212】

SAM105₁～105₄は、セキュアコンテナ104aについては、対応する期間の配信用鍵データKDa₁～KDa₃を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108aおよび利用制御状態データ166aをEMDサービスセンタ102に送信する。

また、SAM105₁～105₄は、セキュアコンテナ104bについては、対応する期間の配信用鍵データKDb₁～KDb₃を用いて復号を行い、所定の署名検証処理などを経てコンテンツの購入形態を決定し、当該決定された購入形態および利用形態などに応じて生成した利用履歴データ108bおよび利用制御状態データ166bをEMDサービスセンタ102に送信する。

【0213】

EMDサービスセンタ102では、利用履歴データ108aに基づいて、コン

テンツプロバイダ101aについての決済請求権データ152aを作成し、これを用いて決済機関91に対して決済処理を行なう。

また、EMDサービスセンタ102では、利用履歴データ108bに基づいて、コンテンツプロバイダ101bについての決済請求権データ152bを作成し、これを用いて決済機関91に対して決済処理を行なう。

【0214】

また、EMDサービスセンタ102は、権利書データ106a, 106bを登録して権威化を行なう。このとき、EMDサービスセンタ102は、権利書データ106a, 106bに対応するキーファイルKF a, KF bに対して、グローバルユニークな識別子Content_IDを配付する。

また、EMDサービスセンタ102は、コンテンツプロバイダ101a, 101bの公開鍵証明書データCER_{cpa}, CER_{cpb}を発行し、これに自らの署名データSIG_{1b,ESC}, SIG_{1a,ESC}を付してその正当性を認証する。

【0215】

第2実施形態

上述した実施形態では、コンテンツプロバイダ101からユーザホームネットワーク103のSAM105₁~105₄にコンテンツデータを直接配給する場合を例示したが、本実施形態では、コンテンツプロバイダが提供するコンテンツデータを、サービスプロバイダを介してユーザホームネットワークのSAMに配給する場合について説明する。

【0216】

図49は、本実施形態のEMDシステム300の構成図である。

図49に示すように、EMDシステム300は、コンテンツプロバイダ301、EMDサービスセンタ302、ユーザホームネットワーク303、サービスプロバイダ310、ペイメントゲートウェイ90および決済機関91を有する。

コンテンツプロバイダ301、EMDサービスセンタ302、SAM305₁~305₄およびサービスプロバイダ310は、それぞれ請求項18および請求項24などに係わるデータ提供装置、管理装置、データ処理装置およびデータ配給装置に対応している。

コンテンツプロバイダ301は、サービスプロバイダ310に対してコンテンツデータを供給する点を除いて、前述した第1実施形態のコンテンツプロバイダ101と同じである。

また、EMDサービスセンタ302は、コンテンツプロバイダ101およびSAM505₁～505₄に加えて、サービスプロバイダ310に対しても認証機能、鍵データ管理機能および権利処理機能を有する点を除いて、前述した第1実施形態のEMDサービスセンタ102と同じである。

また、ユーザホームネットワーク303は、ネットワーク機器360₁およびAV機器360₂～360₄を有している。ネットワーク機器360₁はSAM305₁およびCAモジュール311を内蔵しており、AV機器360₂～360₄はそれぞれSAM305₂～305₄を内蔵している。

ここで、SAM305₁～305₄は、サービスプロバイダ310からセキュアコンテナ304の配給を受ける点と、コンテンツプロバイダ301に加えてサービスプロバイダ310についての署名データの検証処理およびSP用購入履歴データ（データ配給装置用購入履歴データ）309の作成を行なう点とを除いて、前述した第1実施形態のSAM105₁～105₄と同じである。

【0217】

先ず、EMDシステム300の概要について説明する。

EMDシステム300では、コンテンツプロバイダ301は、自らが提供しようとするコンテンツのコンテンツデータCの使用許諾条件などの権利内容を示す前述した第1実施形態と同様の権利書(UCP:Usage Control Policy)データ106を、高い信頼性のある権威機関であるEMDサービスセンタ302に送信する。権利書データ106は、EMDサービスセンタ302に登録されて権威化（認証）される。

【0218】

また、コンテンツプロバイダ301は、コンテンツ鍵データK_cでコンテンツデータCを暗号化してコンテンツファイルCFを生成する。また、コンテンツプロバイダ301は、EMDサービスセンタ302から配給された対応する期間の配信用鍵データKD₁～KD₆を用いて、コンテンツ鍵データK_cおよび権利書

データ106を暗号化し、それらを格納したキーファイルKFを作成する。そして、コンテンツプロバイダ301は、コンテンツファイルCF、キーファイルKFおよび自らの署名データとを格納したセキュアコンテナ104を、インターネットなどのネットワーク、デジタル放送、記録媒体あるいは非公式なプロトコルを用いて、あるいはオフラインなどでサービスプロバイダ310に供給する。

【0219】

サービスプロバイダ310は、コンテンツプロバイダ301からセキュアコンテナ104を受け取ると、署名データの検証を行なって、セキュアコンテナ104が正当なコンテンツプロバイダ301によって作成されたものであるか、並びに送り主の正当性を確認する。

次に、サービスプロバイダ310は、例えばオフラインで通知されたコンテンツプロバイダ301が希望するコンテンツに対しての価格(SRP)に、自らのサービスの価格を加算した価格を示すプライスタグデータ(PT)312を作成する。

そして、サービスプロバイダ310は、セキュアコンテナ104から取り出したコンテンツファイルCFおよびキーファイルKFと、プライスタグデータ312と、これらに対しての自らの秘密鍵データ $K_{SP,S}$ による署名データとを格納したセキュアコンテナ304を作成する。

このとき、キーファイルKFは、配信用鍵データ $KD_1 \sim KD_6$ によって暗号化されており、サービスプロバイダ310は当該配信用鍵データ $KD_1 \sim KD_6$ を保持していないため、サービスプロバイダ310はキーファイルKFの中身を見たり、書き換えたりすることはできない。

また、EMDサービスセンタ302は、プライスタグデータ312を登録して権威化する。

【0220】

サービスプロバイダ310は、オンラインおよび／またはオフラインでセキュアコンテナ304をユーザホームネットワーク303に配給する。

このとき、オフラインの場合には、セキュアコンテナ304は $SAM305_1 \sim 305_4$ にそのまま供給される。一方、オンラインの場合には、サービスプロ

バイダ310とCAモジュール311との間で相互認証を行い、セキュアコンテナ304をサービスプロバイダ310においてセッション鍵データ K_{SES} を用いた暗号化して送信し、CAモジュール311において受信したセキュアコンテナ304をセッション鍵データ K_{SES} を用いて復号した後に、 $SAM305_1 \sim 305_4$ に転送する。

【0221】

次に、 $SAM305_1 \sim 305_4$ において、セキュアコンテナ304を、EMDサービスセンタ302から配給された対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて復号した後に、署名データの検証処理を行う。

$SAM305_1 \sim 305_4$ に供給されたセキュアコンテナ304は、ネットワーク機器360₁およびAV機器360₂～360₄において、ユーザの操作に応じて購入・利用形態が決定された後に、再生や記録媒体への記録などの対象となる。

$SAM305_1 \sim 305_4$ は、上述したセキュアコンテナ304の購入・利用の履歴を利用履歴(Usage Log)データ308として記録する。

利用履歴データ(履歴データまたは管理装置用履歴データ)308は、例えば、EMDサービスセンタ302からの要求に応じて、ユーザホームネットワーク303からEMDサービスセンタ302に送信される。

【0222】

EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、ペイメントゲートウェイ90を介して銀行などの決済機関91に決済を行なう。これにより、ユーザホームネットワーク103のユーザが支払った金銭が、EMDサービスセンタ102による決済処理によって、コンテンツプロバイダ101およびサービスプロバイダ310に分配される。

【0223】

本実施形態では、第1実施形態と同様に、デジタルのコンテンツデータCをカプセル化して提供することで、従来の記録媒体と密着したデジタルコンテンツを

、記録媒体から切り離して、デジタルコンテンツ単体に存在価値を持たせることができる。

ここで、セキュアコンテナは、どのような流通経路（配送チャンネル）を介して提供されても、コンテンツデータC（商品）を販売するときの最も基本となる商品カプセルである。具体的には、セキュアコンテナは、課金を行うための暗号情報や、コンテンツデータCの中身の正当性、コンテンツデータを作成した者の正当性およびコンテンツデータの流通業者の正当性を検証するための署名データや、コンテンツデータに埋め込む電子透かし情報に関する情報などの著作権に係わる情報を含む商品カプセルである。

【 0 2 2 4 】

また、本実施形態では、EMDサービスセンタ302は、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有している。

すなわち、EMDサービスセンタ302は、中立の立場にある最高の権威機関であるルート認証局92に対してのセカンド認証局(Second Certificate Authority)としての役割を果たし、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄において署名データの検証処理に用いられる公開鍵データの公開鍵証明書データに、EMDサービスセンタ302の秘密鍵データによる署名を付けることで、当該公開鍵データの正当性を認証する。また、前述したように、コンテンツプロバイダ301の権利書データ106およびサービスプロバイダ310のプライスタグデータ312を登録して権威化することも、EMDサービスセンタ302の認証機能によるものである。

また、EMDサービスセンタ302は、例えば、配信用鍵データKD₁～KD₆などの鍵データの管理を行なう鍵データ管理機能を有する。

また、EMDサービスセンタ302は、コンテンツプロバイダ301が登録した権利書データ106とSAM305₁～SAM305₄から入力した利用履歴データ308とサービスプロバイダ310が登録したプライスタグデータ312とに基づいて、ユーザホームネットワーク303のユーザによるコンテンツの購入・利用に対して決済を行い、ユーザが支払った金銭をコンテンツプロバイダ301およびサービスプロバイダ310に分配して支払う権利処理（利益分配）機

能を有する。

【0225】

以下、コンテンツプロバイダ301の各構成要素について詳細に説明する。

〔コンテンツプロバイダ301〕

図50は、コンテンツプロバイダ301の機能ブロック図であり、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されている。

図50に示すように、コンテンツプロバイダ301は、コンテンツマスターサーバ111、電子透かし情報付加部112、圧縮部113、暗号化部114、乱数発生部115、暗号化部116、署名処理部117、セキュアコンテナ作成部118、セキュアコンテナデータベース118a、記憶部119、相互認証部120、暗号化・復号部121、権利書データ作成部122、EMDサービスセンタ管理部125およびサービスプロバイダ管理部324を有する。

【0226】

図50において、図2と同一符号を付した構成要素は、前述した第1実施形態において図2および図3を参照しながら説明した同一符号の構成要素と同じである。

すなわち、コンテンツプロバイダ301は、図2に示すSAM管理部124の代わりにサービスプロバイダ管理部324を設けた構成をしている。

サービスプロバイダ管理部324は、セキュアコンテナ作成部118から入力したセキュアコンテナ104を、オフラインおよび／またはオンラインで、図49に示すサービスプロバイダ310に提供する。セキュアコンテナ104には、第1実施形態と同様に、図4(A)，(B)，(C)に示すコンテンツファイルCFおよびその署名データSIG_{6,CP}と、キーファイルKFおよびその署名データSIG_{7,CP}と、公開鍵証明書データCER_{CP}およびその署名データSIG_{1,ESC}とが格納されている。

【0227】

サービスプロバイダ管理部324は、セキュアコンテナ104をオンラインでサービスプロバイダ310に配信する場合には、暗号化・復号部121において

セッション鍵データ K_{SES} を用いてセキュアコンテナ104を暗号化した後に、ネットワークを介してサービスプロバイダ310に配信する。

【0228】

また、図3に示したコンテンツプロバイダ101内でのデータの流れは、サービスプロバイダ310にも同様に適用される。

【0229】

〔サービスプロバイダ310〕

サービスプロバイダ310は、コンテンツプロバイダ301から提供を受けたセキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFと、自らが生成したプライスタグデータ312とを格納したセキュアコンテナ304を、オンラインおよび／またはオフラインで、ユーザホームネットワーク303のネットワーク機器360₁ およびAV機器360₂ ~ 360₄ に配給する。

サービスプロバイダ310によるコンテンツ配給のサービス形態には、大きく分けて、独立型サービスと連動型サービスとがある。

独立型サービスは、例えば、コンテンツを個別に配給するダウンロード専用のサービスである。また、連動型サービスは、番組、CM（広告）に連動してコンテンツを配給するサービスであり、例えば、ドラマ番組のストリーム内にドラマの主題歌や挿入歌のコンテンツが格納してある。ユーザは、ドラマ番組を見ているときに、そのストリーム中にある主題歌や挿入歌のコンテンツを購入できる。

【0230】

図51は、サービスプロバイダ310の機能ブロック図である。

なお、図51には、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104に応じたセキュアコンテナ304をユーザホームネットワーク303に供給する際のデータの流れが示されている。

図51に示すように、サービスプロバイダ310は、コンテンツプロバイダ管理部350、記憶部351、相互認証部352、暗号化・復号部353、署名処理部354、セキュアコンテナ作成部355、セキュアコンテナデータベース355a、プライスタグデータ作成部356、ユーザホームネットワーク管理部357、EMDサービスセンタ管理部358およびユーザ嗜好フィルタ生成部92

0を有する。

【0231】

以下、コンテンツプロバイダ301から供給を受けたセキュアコンテナ104からセキュアコンテナ304を作成し、これをユーザホームネットワーク303に配給する際のサービスプロバイダ310内での処理の流れを図51および図52を参照しながら説明する。

図52は、当該処理のフローチャートである。

ステップSZ1：コンテンツプロバイダ管理部350は、オンラインおよび／またはオフラインで、コンテンツプロバイダ301から図4に示すセキュアコンテナ104の供給を受けてセキュアコンテナ104を記憶部351に書き込む。

このとき、コンテンツプロバイダ管理部350は、オンラインの場合には、図50に示す相互認証部120と図51に示す相互認証部352との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて、セキュアコンテナ104を暗号化・復号部353において復号した後に、記憶部351に書き込む。

【0232】

ステップSZ2：署名処理部354において、記憶部351に記憶されているセキュアコンテナ104の図4(C)に示す署名データ $SIG_{1,ESC}$ を、記憶部351から読み出したEMDサービスセンタ302の公開鍵データ $K_{ESC,P}$ を用いて検証し、その正当性が認められた後に、図4(C)に示す公開鍵証明書データ CER_{CP} から公開鍵データ $K_{CP,P}$ を取り出す。

ステップSZ3：署名処理部354は、当該取り出した公開鍵データ $K_{CP,P}$ を用いて、記憶部351に記憶されているセキュアコンテナ104の図4(A)，(B)に示す署名データ $SIG_{6,CP}$ 、 $SIG_{7,CP}$ の検証を行う。

【0233】

ステップSZ4：プライスタグデータ作成部356は、例えばコンテンツプロバイダ301からオフラインで通知されたコンテンツプロバイダ301が要求するコンテンツに対しての価格に、自らのサービスの価格を加算した価格を示すプライスタグデータ312を作成し、これをセキュアコンテナ作成部355に出力する。

【0234】

ステップSZ5：署名処理部354は、コンテンツファイルCF、キーファイルKFおよびプライスタグデータ312のハッシュ値をとり、サービスプロバイダ310の秘密鍵データ $K_{SP,P}$ を用いて、署名データ $SIG_{62,SP}$ 、 $SIG_{63,SP}$ 、 $SIG_{64,SP}$ を作成し、これをセキュアコンテナ作成部355に出力する。

【0235】

ステップSZ6：セキュアコンテナ作成部355は、図53(A)～(D)に示すように、コンテンツファイルCFおよびその署名データ $SIG_{62,SP}$ と、キーファイルKFおよびその署名データ $SIG_{63,ESC}$ と、プライスタグデータ312およびその署名データ $SIG_{64,SP}$ と、公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61,ESC}$ とを格納したセキュアコンテナ304を作成し、セキュアコンテナデータベース355aに格納する。そして、セキュアコンテナ作成部355は、ユーザホームネットワーク303からの要求に応じたセキュアコンテナ304をセキュアコンテナデータベース355aから読み出してユーザホームネットワーク管理部357に出力する。

このとき、セキュアコンテナ304は、複数のコンテンツファイルCFと、それらにそれぞれ対応した複数のキーファイルKFとを格納した複合コンテナであってもよい。例えば、単数のセキュアコンテナ304内に、それぞれ曲、ビデオクリップ、歌詞カード、ライナーノーツおよびジャケットに関する複数のコンテンツファイルCFを単数のセキュアコンテナ304に格納してもよい。これらの複数のコンテンツファイルCFなどは、ディレクトリー構造でセキュアコンテナ304内に格納してもよい。

【0236】

また、セキュアコンテナ304は、デジタル放送で送信される場合には、MH EG (Multimedia and Hypermedia information coding Experts Group) プロトコルが用いられ、インターネットで送信される場合にはXML / SMIL / HTML (Hyper TextMarkup Language) プロトコルが用いられる。

このとき、コンテンツファイルCFおよびキーファイルKFは、コンテンツプロバイダ301によって一元的に管理され、セキュアコンテナ304を送信する

プロトコルに依存しない。すなわち、コンテンツファイルCFおよびキーファイルKFは、MHEGおよびHTMLのプロトコルをトンネリングした形でセキュアコンテナ304内に格納される。

【0237】

ステップSZ7：ユーザホームネットワーク管理部357は、セキュアコンテナ304を、オフラインおよび／またはオンラインでユーザホームネットワーク303に供給する。

ユーザホームネットワーク管理部357は、セキュアコンテナ304をオンラインでユーザホームネットワーク303のネットワーク機器360₁に配信する場合には、相互認証後に、暗号化・復号部352においてセッション鍵データK_{SES}を用いてセキュアコンテナ304を暗号化した後に、ネットワークを介してネットワーク機器360₁に配信する。

【0238】

なお、ユーザホームネットワーク管理部357は、セキュアコンテナ304を例えば衛星などを介して放送する場合には、セキュアコンテナ304をスクランブル鍵データK_{SCR}を用いて暗号化する。また、スクランブル鍵データK_{SCR}をワーク鍵データK_Wを暗号化し、ワーク鍵データK_Wをマスタ鍵データK_Mを用いて暗号化する。

そして、ユーザホームネットワーク管理部357は、セキュアコンテナ304と共に、スクランブル鍵データK_{SCR}およびワーク鍵データK_Wを、衛星を介してユーザホームネットワーク303に送信する。

また、例えば、マスタ鍵データK_Mを、ICカードなどに記憶してオフラインでユーザホームネットワーク303に配給する。

【0239】

また、ユーザホームネットワーク管理部357は、ユーザホームネットワーク303から、当該サービスプロバイダ310が配給したコンテンツデータCについてのSP用購入履歴データ309を受信すると、これを記憶部351に書き込む。

サービスプロバイダ310は、将来のサービス内容を決定する際に、SP用購

入履歴データ309を参照する。また、ユーザ嗜好フィルタ生成部920は、SP用購入履歴データ309に基づいて、当該SP用購入履歴データ309を送信したSAM305₁～305₄のユーザの嗜好を分析してユーザ嗜好フィルタデータ900を生成し、これをユーザホームネットワーク管理部357を介してユーザホームネットワーク303のCAモジュール311に送信する。

【0240】

図54には、サービスプロバイダ310内におけるEMDサービスセンタ302との間の通信に関連するデータの流れが示されている。

なお、以下に示す処理を行う前提として、サービスプロバイダ310の関係者は、例えば、自らの身分証明書および決済処理を行う銀行口座などを用いて、オフラインで、EMDサービスセンタ302に登録処理を行い、グローバルユニークな識別子SP_IDを得ている。識別子SP_IDは、記憶部351に記憶される。

【0241】

まず、サービスプロバイダ310が、EMDサービスセンタ302に、自らの秘密鍵データ $K_{SP,S}$ に対応する公開鍵データ $K_{SP,S}$ の正当性を証明する公開鍵証明書データ CER_{SP} を要求する場合の処理を図54を参照しながら説明する。

まず、サービスプロバイダ310は、真性乱数発生器を用いて乱数を発生して秘密鍵データ $K_{SP,S}$ を生成し、当該秘密鍵データ $K_{SP,S}$ に対応する公開鍵データ $K_{SP,P}$ を作成して記憶部351に記憶する。

EMDサービスセンタ管理部358、サービスプロバイダ310の識別子SP_IDおよび公開鍵データ $K_{SP,P}$ を記憶部351から読み出す。

そして、EMDサービスセンタ管理部358は、識別子SP_IDおよび公開鍵データ $K_{SP,P}$ を、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ管理部348は、当該登録に応じて、公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61,ESC}$ をEMDサービスセンタ302から入力して記憶部351に書き込む。

【0242】

次に、サービスプロバイダ310が、EMDサービスセンタ302にプライス

タグデータ 312 を登録して権威化する場合の処理を図 54 を参照して説明する。

【0243】

この場合には、署名処理部 354 において、プライスタグデータ作成部 356 が作成したプライスタグデータ 312 と記憶部 351 から読み出したグローバルユニークな識別子 $Content_ID$ とを格納したモジュール Mod_{103} のハッシュ値が求められ、秘密鍵データ $K_{SP,S}$ を用いて署名データ $SIG_{80,SP}$ が生成される。

また、記憶部 351 から公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61,ESC}$ が読み出される。

そして、図 55 に示すプライスタグ登録要求用モジュール Mod_{102} を、相互認証部 352 と EMD サービスセンタ 302 との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて暗号化・復号部 353 において暗号化した後に、EMD サービスセンタ管理部 358 から EMD サービスセンタ 302 に送信する。

なお、モジュール Mod_{103} に、サービスプロバイダ 310 のグローバルユニークな識別子 SP_ID を格納してもよい。

【0244】

また、EMD サービスセンタ管理部 358 は、EMD サービスセンタ 302 から受信した決済レポートデータ 307s を記憶部 351 に書き込む。

【0245】

また、EMD サービスセンタ管理部 358 は、EMD サービスセンタ 302 から受信したマーケティング情報データ 904 を記憶部 351 に記憶する。

マーケティング情報データ 904 は、サービスプロバイダ 310 が今後配給するコンテンツデータ C を決定する際に参考にされる。

【0246】

[EMD サービスセンタ 302]

EMD サービスセンタ 302 は、前述したように、認証局 (CA: Certificate Authority)、鍵管理 (Key Management) 局および権利処理 (Rights Clearing) 局

としての役割を果たす。

図56は、EMDサービスセンタ302の機能の構成図である。

図56に示すように、EMDサービスセンタ302は、鍵サーバ141、鍵データベース141a、決済処理部442、署名処理部443、決算機関管理部144、証明書・権利書管理部445、CERデータベース445a、コンテンツプロバイダ管理部148、CPデータベース148a、SAM管理部149、SAMデータベース149a、相互認証部150、暗号化・復号部151、サービスプロバイダ管理部390、SPデータベース390a、ユーザ嗜好フィルタ生成部901およびマーケティング情報データ生成部902を有する。

図56において、図1.0および図1.1と同じ符号を付した機能ブロックは、第1実施形態で説明した同一符号の機能ブロックと略同じ機能を有している。

以下、図56において、新たな符号を付した機能ブロックについて説明する。

なお、図56には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、サービスプロバイダ310との間で送受信されるデータに関連するデータの流れが示されている。

また、図57には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、コンテンツプロバイダ301との間で送受信されるデータに関連するデータの流れが示されている。

また、図58には、EMDサービスセンタ302内の機能ブロック相互間のデータの流れのうち、図4.9に示すSAM305₁～305₄および決済機関91との間で送受信されるデータに関連するデータの流れが示されている。

【0247】

決済処理部442は、図58に示すように、SAM305₁～305₄から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312に基づいて決済処理を行う。なお、この際に、決済処理部442は、サービスプロバイダ310によるダンピングの有無などを監視する。

決済処理部442は、決済処理により、図58に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ1

52cを作成し、これらをそれぞれコンテンツプロバイダ管理部148および決算機関管理部144に出力する。

また、決済処理により、図56および図58に示すように、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sを作成し、これらをそれぞれサービスプロバイダ管理部390および決算機関管理部144に出力する。

ここで、決済請求権データ152c, 152sは、当該データに基づいて、決済機関91に金銭の支払いを請求できる権威化されたデータである。

【0248】

ここで、利用履歴データ308は、第1実施形態で説明した利用履歴データ108と同様に、セキュアコンテナ304に関連したライセンス料の支払いを決定する際に用いられる。利用履歴データ308には、例えば、図59に示すように、セキュアコンテナ304に格納されたコンテンツデータCの識別子Content_ID、セキュアコンテナ304に格納されたコンテンツデータCを提供したコンテンツプロバイダ301の識別子CP_ID、セキュアコンテナ304を配給したサービスプロバイダ310の識別子SP_ID、コンテンツデータCの信号諸元データ、セキュアコンテナ304内のコンテンツデータCの圧縮方法、セキュアコンテナ304を記録した記録媒体の識別子Media_ID、セキュアコンテナ304を配給を受けたSAM305₁～305₄の識別子SAM_ID、当該SAM105₁～105₄のユーザのUSER_IDなどが記述されている。従って、EMDサービスセンタ302は、コンテンツプロバイダ301およびサービスプロバイダ310の所有者以外にも、例えば、圧縮方法や記録媒体などのライセンス所有者に、ユーザホームネットワーク303のユーザが支払った金銭を分配する必要がある場合には、予め決められた分配率表に基づいて各相手に支払う金額を決定し、当該決定に応じた決済レポートデータおよび決済請求権データを作成する。

【0249】

証明書・権利書管理部445は、CERデータベース445aに登録されて権威化された公開鍵証明書データCER_{cp}、公開鍵証明書データCER_{sp}および公

開鍵証明書データ $CER_{SAM1} \sim CER_{SAM2}$ などを読み出すと共に、コンテンツプロバイダ 301 の権利書データ 106 およびコンテンツ鍵データ K_c 、並びにサービスプロバイダ 310 のプライスタグデータ 312 などを CER データベース 445a に登録して権威化する。

このとき、証明書・権利書管理部 445 は、権利書データ 106、コンテンツ鍵データ K_c およびプライスタグデータ 312 などのハッシュ値をとり、秘密鍵データ $K_{ESC,S}$ を用いた署名データを付して権威化証明書データを作成する。

【0250】

コンテンツプロバイダ管理部 148 は、コンテンツプロバイダ 101 との間で通信する機能を有し、登録されているコンテンツプロバイダ 101 の識別子 CP_ID などを管理する CP データベース 148a にアクセスできる。

【0251】

ユーザ嗜好フィルタ生成部 901 は、利用履歴データ 308 に基づいて、当該利用履歴データ 308 を送信した $SAM305_1 \sim 305_4$ のユーザの嗜好に応じたコンテンツデータ C を選択するためのユーザ嗜好フィルタデータ 903 を生成し、ユーザ嗜好フィルタデータ 903 を SAM 管理部 149 を介して、当該利用履歴データ 308 を送信した $SAM305_1 \sim 305_4$ に送信する。

【0252】

マーケティング情報データ生成部 902 は、利用履歴データ 308 に基づいて、例えば、複数のサービスプロバイダ 310 によってユーザホームネットワーク 103 に配給されたコンテンツデータ C の全体の購入状況などを示すマーケティング情報データ 904 を生成し、これをサービスプロバイダ管理部 390 を介して、サービスプロバイダ 310 に送信する。サービスプロバイダ 310 は、マーケティング情報データ 904 を参考にして、今後提供するサービスの内容を決定する。

【0253】

以下、EMD サービスセンタ 302 内での処理の流れを説明する。

EMD サービスセンタ 302 からコンテンツプロバイダ 301 への配信用鍵データ $KD_1 \sim KD_6$ の送信と、EMD サービスセンタ 302 から $SAM305_1$

～305₄ への配信用鍵データ $KD_1 \sim KD_3$ の送信とは、第1実施形態の場合と同様に行なわれる。

【0254】

また、EMDサービスセンタ302がコンテンツプロバイダ301から、公開鍵証明書データの発行要求を受けた場合の処理も、証明書・権利書管理部445がCERデータベース445aに対して登録を行なう点を除いて、前述した第1実施形態の場合と同様に行なわれる。

【0255】

以下、EMDサービスセンタ302がサービスプロバイダ310から、公開鍵証明書データの発行要求を受けた場合の処理を、図56および図60を参照しながら説明する。

図60は、当該処理のフローチャートである。

ステップS01：サービスプロバイダ管理部390は、予めEMDサービスセンタ302によって与えられたサービスプロバイダ310の識別子 SP_ID 、公開鍵データ $K_{SP,P}$ および署名データ $SIG_{70,SP}$ を含む公開鍵証明書データ登録要求をサービスプロバイダ310から受信すると、これらを、相互認証部150と図51に示す相互認証部352と間の相互認証で得られたセッション鍵データ K_{SES} を用いて復号する。

【0256】

ステップS02：当該復号した署名データ $SIG_{70,SP}$ の正当性を署名処理部443において確認した後に、識別子 SP_ID および公開鍵データ $K_{SP,P}$ に基づいて、当該公開鍵証明書データの発行要求を出したサービスプロバイダ310がSPデータベース390aに登録されているか否かを確認する。

ステップS03：証明書・権利書管理部445は、当該サービスプロバイダ310の公開鍵証明書データ CER_{SP} をCERデータベース445aから読み出してサービスプロバイダ管理部390に出力する。

【0257】

ステップS04：署名処理部443は、公開鍵証明書データ CER_{SP} のハッシュ値をとり、EMDサービスセンタ302の秘密鍵データ $K_{ESC,S}$ を用いて、署

名データ $SIG_{61,ESC}$ を作成し、これをサービスプロバイダ管理部390に出力する。

ステップS05：サービスプロバイダ管理部390は、公開鍵証明書データ CER_{SP} およびその署名データ $SIG_{61,ESC}$ を、相互認証部150と図51に示す相互認証部352と間の相互認証で得られたセッション鍵データ K_{SES} を用いて暗号化した後に、サービスプロバイダ310に送信する。

【0258】

なお、EMDサービスセンタ302が $SAM105_1 \sim 105_4$ から、公開鍵証明書データの発行要求を受けた場合の処理は、第1実施形態と同様である。

また、EMDサービスセンタ302が、コンテンツプロバイダ301から権利書データ106の登録要求を受けた場合の処理も、第1実施形態と同様である。

【0259】

次に、EMDサービスセンタ302が、サービスプロバイダ310からプライスタグデータ312の登録要求を受けた場合の処理を、図56および図61を参照しながら説明する。

図61は、当該処理のフローチャートである。

ステップSP1：サービスプロバイダ管理部390がサービスプロバイダ310から図55に示すプライスタグ登録要求モジュール Mod_{102} を受信すると、相互認証部150と図51に示す相互認証部352との間の相互認証で得られたセッション鍵データ K_{SES} を用いてプライスタグ登録要求モジュール Mod_{102} を復号する。

【0260】

ステップSP2：当該復号したプライスタグ登録要求モジュール Mod_{102} に格納された署名データ $SIG_{80,SP}$ の正当性を署名処理部443において確認する。

【0261】

ステップSP3：証明書・権利書管理部445は、プライスタグ登録要求モジュール Mod_{102} に格納されたプライスタグデータ312を、CERデータベース445aに登録して権威化する。

【0262】

次に、EMDサービスセンタ302において決済を行なう場合の処理を図58および図62を参照しながら説明する。

図62は、当該処理のフローチャートである。

ステップSQ1：SAM管理部149は、ユーザホームネットワーク303の例えばSAM305₁から利用履歴データ308およびその署名データSIG_{205,SAM1}を入力すると、利用履歴データ308および署名データSIG_{205,SAM1}を、相互認証部150とSAM305₁～305₄との間の相互認証によって得られたセッション鍵データK_{SES}を用いて復号し、SAM305₁の公開鍵データK_{SAM1,p}を用いて署名データSIG_{205,SAM1}の検証を行なった後に、決算処理部442に出力する。

【0263】

ステップSQ2：決済処理部442は、SAM305₁から入力した利用履歴データ308と、証明書・権利書管理部445から入力した標準小売価格データSRPおよびプライスタグデータ312とに基づいて決済処理を行う。

決済処理部442は、決済処理により、図58に示すように、コンテンツプロバイダ301についての決済レポートデータ307cおよび決済請求権データ152cと、サービスプロバイダ310についての決済レポートデータ307sおよび決済請求権データ152sとを作成する。

なお、決済処理部442による決済処理は、利用履歴データ308を入力する毎に行ってもよいし、所定の期間毎に行ってもよい。

【0264】

ステップSQ3：図56および図58に示すように、コンテンツプロバイダ301およびサービスプロバイダ310についての決済請求権データ152c、152sを作成し、これらを決算機関管理部144に出力する。

決算機関管理部144は、決済請求権データ152c、152sと、それらについて秘密鍵データK_{ESC,S}を用いて作成した署名データとを、相互認証およびセッション鍵データK_{SES}による復号を行なった後に、図49に示すペイメントゲートウェイ90を介して決済機関91に送信する。

これにより、決済請求権データ152cに示される金額の金銭がコンテンツプロバイダ301に支払われ、決済請求権データ152sに示される金額の金銭がサービスプロバイダ310に支払われる。

なお、EMDサービスセンタ302は、決済請求権データ152c, 152sをそれぞれコンテンツプロバイダ301およびサービスプロバイダ310に送信してもよい。この場合には、コンテンツプロバイダ301およびサービスプロバイダ310が、当該受信した決済請求権データ152c, 152sに基づいて決済機関91に金銭を請求する。

【0265】

ステップSQ4：コンテンツプロバイダ301およびサービスプロバイダ310についての決済レポートデータS307c, S307sが、それぞれコンテンツプロバイダ管理部148およびサービスプロバイダ管理部390を介して、コンテンツプロバイダ301およびサービスプロバイダ310に出力される。

【0266】

EMDサービスセンタ302は、その他に、第1実施形態のEMDサービスセンタ102と同様に、SAM305₁～305₄の出荷時の処理と、SAM登録リストの登録処理とを行なう。

【0267】

〔ユーザホームネットワーク303〕

ユーザホームネットワーク303は、図49に示すように、ネットワーク機器360₁およびA/V機器360₂～360₄を有している。

ネットワーク機器360₁は、CAモジュール311およびSAM305₁を内蔵している。また、AV機器360₂～360₄は、それぞれSAM305₂～305₄を内蔵している。

SAM305₁～305₄の相互間は、例えば、1394シリアルインタフェースバスなどのバス191を介して接続されている。

なお、AV機器360₂～360₄は、ネットワーク通信機能を有していてもよいし、ネットワーク通信機能を有しておらず、バス191を介してネットワーク機器360₁のネットワーク通信機能を利用してもよい。

また、ユーザホームネットワーク303は、ネットワーク機能を有していないAV機器のみを有していてもよい。

【0268】

以下、ネットワーク機器360₁について説明する。

図63は、ネットワーク機器360₁の構成図である。

図63に示すように、ネットワーク機器360₁は、通信モジュール162、CAモジュール311、復号モジュール905、SAM305₁、復号・伸長モジュール163、購入・利用形態決定操作部165、ダウンロードメモリ167、再生モジュール169および外部メモリ201を有する。

図63において、図16と同一符号を付した構成要素は、第1実施形態で説明した同一符号の構成要素と同じである。

【0269】

通信モジュール162は、サービスプロバイダ310との間の通信処理を行う。

具体的には、通信モジュール162は、サービスプロバイダ310から衛星放送などで受信したセキュアコンテンツ304を復号モジュール905に出力する。また、通信モジュール162は、サービスプロバイダ310に電話回線などを介してSP用購入履歴データ309を受信したユーザ嗜好フィルタデータ900をCAモジュール311に出力すると共に、CAモジュール311から入力したSP用購入履歴データ309を電話回線などを介してサービスプロバイダ310に送信する。

【0270】

図64は、CAモジュール311および復号モジュール905の機能ブロック図である。

図64に示すように、CAモジュール311は、相互認証部906、記憶部907、暗号化・復号部908およびSP用購入履歴データ生成部909を有する。

相互認証部906は、CAモジュール311とサービスプロバイダ310との間で電話回線を介してデータを送受信する際に、サービスプロバイダ310との

間で相互認証を行ってセッション鍵データ K_{SES} を生成し、これを暗号化・復号部908に出力する。

【0271】

記憶部907は、例えば、サービスプロバイダ310とユーザとの間で契約が成立した後に、サービスプロバイダ310からICカード912などを用いてオフラインで供給されたマスタ鍵データ K_M を記憶する。

【0272】

暗号化・復号部908は、復号モジュール905の復号部910からそれぞれ暗号化されたスクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を入力し、記憶部907から読み出したマスタ鍵データ K_M を用いてワーク鍵データ K_W を復号する。そして、暗号化・復号部908は、当該復号したワーク鍵データ K_W を用いてスクランブル鍵データ K_{SCR} を復号し、当該復号したスクランブル鍵データ K_{SCR} を復号部910に出力する。

また、暗号化・復号部908は、電話回線などを介して通信モジュール162がサービスプロバイダ310から受信したユーザ嗜好フィルタデータ900を、相互認証部906からのセッション鍵データ K_{SES} を用いて復号して復号モジュール905のセキュアコンテンツ選択部911に出力する。

また、暗号化・復号部908は、SP用購入履歴データ生成部909から入力したSP用購入履歴データ309を、相互認証部906からのセッション鍵データ K_{SES} を用いて復号して通信モジュール162を介してサービスプロバイダ310に送信する。

【0273】

SP用購入履歴データ生成部909は、図63に示す購入・利用形態決定操作部165を用いてユーザによるコンテンツデータCの購入操作に応じた操作信号S165、またはSAM305₁からの利用制御状態データ166に基づいて、サービスプロバイダ310に固有のコンテンツデータCの購入履歴を示すSP用購入履歴データ309を生成し、これを暗号化・復号部908に出力する。

SP用購入履歴データ309は、例えば、サービスプロバイダ310が配信サービスに関してユーザから徴収したい情報、月々の基本料金（ネットワーク家賃

）、契約（更新）情報および購入履歴情報などを含む。

【0274】

なお、CAモジュール311は、サービスプロバイダ310が課金機能を有している場合には、サービスプロバイダ310の課金データベース、顧客管理データベースおよびマーケティング情報データベースと通信を行う。この場合に、CAモジュール311は、コンテンツデータの配信サービスについての課金データをサービスプロバイダ310に送信する。

【0275】

復号モジュール905は、復号部910およびセキュアコンテナ選択部911を有する。

復号部910は、通信モジュール162から、それぞれ暗号化されたセキュアコンテナ304、スクランブル鍵データ K_{SCR} およびワーク鍵データ K_W を入力する。

そして、復号部910は、暗号化されたスクランブル鍵データ K_{SCR} およびワーク鍵データ K_W をCAモジュール311の暗号化・復号部908に出力し、暗号化・復号部908から復号されたスクランブル鍵データ K_{SCR} を入力する。

そして、復号部910は、暗号化されたセキュアコンテナ304を、スクランブル鍵データ K_{SCR} を用いて復号した後に、セキュアコンテナ選択部911に出力する。

【0276】

なお、セキュアコンテナ304が、MPEG2 Transport Stream 方式でサービスプロバイダ310から送信される場合には、例えば、復号部910は、TS Packet 内のECM(Entitlement Control Message) からスクランブル鍵データ K_{SCR} を取り出し、EMM(Entitlement Management Message)からワーク鍵データ K_W を取り出す。

ECMには、その他に、例えば、チャンネル毎の番組属性情報などが含まれている。また、EMMは、その他に、ユーザ（視聴者）毎に異なる個別試聴契約情報などが含まれている。

【0277】

セキュアコンテナ選択部911は、復号部910から入力したセキュアコンテナ304を、CAモジュール311から入力したユーザ嗜好フィルタデータ900を用いてフィルタリング処理して、ユーザの嗜好に応じたセキュアコンテナ304を選択してSAM305₁に出力する。

【0278】

次に、SAM305₁について説明する。

なお、SAM305₁は、サービスプロバイダ310についての署名検証処理を行なうなど、コンテンツプロバイダ301に加えてサービスプロバイダ310に関しての処理を行う点を除いて、図17～図41を用いて前述した第1実施形態のSAM105₁と基本的に行なう機能および構造を有している。

また、SAM305₂～305₄は、SAM305₁と基本的に同じ機能を有している。

すなわち、SAM305₁～305₄は、コンテンツ単位の課金処理をおこなうモジュールであり、EMDサービスセンタ302との間で通信を行う。

【0279】

以下、SAM305₁の機能について詳細に説明する。

図65は、SAM305₁の機能の構成図である。

なお、図65には、サービスプロバイダ310からセキュアコンテナ304を入力し、セキュアコンテナ304内のキーファイルKFを復号する処理に関連するデータの流れが示されている。

図65に示すように、SAM305₁は、相互認証部170、暗号化・復号部171、172、173、誤り訂正部181、ダウンロードメモリ管理部182、セキュアコンテナ復号部183、復号・伸長モジュール管理部184、EMDサービスセンタ管理部185、利用監視部186、署名処理部189、SAM管理部190、記憶部192、メディアSAM管理部197、スタックメモリ200、サービスプロバイダ管理部580、課金処理部587、署名処理部598および外部メモリ管理部811を有する。

なお、図65に示すSAM305₁の所定の機能は、SAM105₁の場合と

同様に、CPUにおいて秘密プログラムを実行することによって実現される。

図65において、図17と同じ符号を付した機能ブロックは、第1実施形態で説明した同一符号の機能ブロックと同じである。

【0280】

また、図63に示す外部メモリ201には、第1実施形態で説明した処理および後述する処理を経て、利用履歴データ308およびSAM登録リストが記憶される。

また、スタックメモリ200には、図66に示すように、コンテンツ鍵データ K_c 、権利書データ(UCP)106、記憶部192のロック鍵データ K_{LOC} 、コンテンツプロバイダ301の公開鍵証明書データ CER_{CP} 、サービスプロバイダ310の公開鍵証明書データ CER_{SP} 、利用制御状態データ(UCS)366、SAMプログラム・ダウンロード・コンテナ $SDC_1 \sim SDC_3$ およびプライスタグデータ312などが記憶される。

【0281】

以下、SAM305₁の機能ブロックのうち、図65において新たに符号を付した機能ブロックについて説明する。

署名処理部589は、記憶部192あるいはスタックメモリ200から読み出したEMDサービスセンタ302の公開鍵データ $K_{ESC,P}$ 、コンテンツプロバイダ301の公開鍵データ $K_{cp,p}$ およびサービスプロバイダ310の公開鍵データ $K_{sp,p}$ を用いて、セキュアコンテナ304内の署名データの検証を行なう。

【0282】

課金処理部587は、図67に示すように、図63に示す購入・利用形態決定操作部165からの操作信号S165と、スタックメモリ200から読み出されたプライスタグデータ312とに基づいて、ユーザによるコンテンツの購入・利用形態に応じた課金処理を行う。

課金処理部587による課金処理は、利用監視部186の監視の下、権利書データ106が示す使用許諾条件などの権利内容および利用制御状態データ166に基づいて行われる。すなわち、ユーザは、当該権利内容などに従った範囲内でコンテンツの購入および利用を行うことができる。

【0283】

また、課金処理部587は、課金処理において、利用履歴データ308を生成し、これを外部メモリ管理部811を介して外部メモリ201に書き込む。

ここで、利用履歴データ308は、第1実施形態の利用履歴データ108と同様に、EMDサービスセンタ302において、セキュアコンテナ304に関連したライセンス料の支払いを決定する際に用いられる。

【0284】

また、課金処理部587は、操作信号S165に基づいて、ユーザによるコンテンツの購入・利用形態を記述した利用制御状態 (UCS: Usage Control Status) データ166を生成し、これを外部メモリ管理部811を介して外部メモリ201に書き込む。

コンテンツの購入形態としては、例えば、購入者による再生や当該購入者の利用のための複製に制限を加えない買い切りや、再生する度に課金を行なう再生課金などがある。

ここで、利用制御状態データ166は、ユーザがコンテンツの購入形態を決定したときに生成され、以後、当該決定された購入形態で許諾された範囲内でユーザが当該コンテンツの利用を行なうように制御するために用いられる。利用制御状態データ166には、コンテンツのID、購入形態、買い切り価格、当該コンテンツの購入が行なわれたSAMのSAM_ID、購入を行なったユーザのUSER_IDなどが記述されている。

【0285】

なお、決定された購入形態が再生課金である場合には、例えば、SAM305₁からサービスプロバイダ310に利用制御状態データ166をリアルタイムに送信し、サービスプロバイダ310がEMDサービスセンタ302に、利用履歴データ108をSAM105₁に取りに行くことを指示する。

また、決定された購入形態が買い切りである場合には、例えば、利用制御状態データ166が、サービスプロバイダ310およびEMDサービスセンタ302にリアルタイムに送信される。

【0286】

また、SAM305₁では、EMDサービスセンタ管理部185がEMDサービスセンタ302から受信したユーザ嗜好フィルタデータ903が、サービスプロバイダ管理部580に出力される。そして、サービスプロバイダ管理部580において、図63に示す復号モジュール905から入力したセキュアコンテナ304が、ユーザ嗜好フィルタデータ903に基づいてフィルタリングされてユーザの嗜好に応じたセキュアコンテナ304が選択され、当該選択されたセキュアコンテナ304が誤り訂正部181に出力される。これにより、SAM305₁において、当該SAM305₁のユーザが契約している全てのサービスプロバイダ310を対象として、当該ユーザによるコンテンツデータCの購入状況から得られた当該ユーザの嗜好に基づいたコンテンツデータCの選択処理が可能になる。

【0287】

以下、SAM305₁内での処理の流れを説明する。

EMDサービスセンタ302から受信した配信用鍵データKD₁～KD₃を記憶部192に格納する際のSAM305₁内での処理の流れは、前述したSAM105₁の場合と同様である。

【0288】

以下、セキュアコンテナ304をサービスプロバイダ310から入力し、セキュアコンテナ304内のキーファイルKFを復号する際のSAM305₁内での処理の流れを図65および図68を参照しながら説明する。

図68は、当該処理のフローチャートである。

ステップSR1：相互認証部170と図51に示すサービスプロバイダ310の相互認証部352との間で相互認証が行なわれる。

暗号化・復号部171は、当該相互認証によって得られたセッション鍵データK_{SES}を用いて、サービスプロバイダ管理部580を介してサービスプロバイダ310から受信した図53に示すセキュアコンテナ304を復号する。

【0289】

ステップSR2：署名処理部589は、図53(D)に示す署名データSIG

61,ESCの検証を行なった後に、図53 (D) に示す公開鍵証明書データ CER_{SP} 内に格納されたサービスプロバイダ310の公開鍵データ $K_{SP,P}$ を用いて、署名データ $SIG_{62,SP}$ 、 $SIG_{63,SP}$ 、 $SIG_{64,SP}$ の正当性を確認する。

サービスプロバイダ管理部580は、署名データ $SIG_{62,SP}$ 、 $SIG_{63,SP}$ 、 $SIG_{64,SP}$ の正当性が確認されると、セキュアコンテナ304を誤り訂正部181に出力する。

誤り訂正部181は、セキュアコンテナ304を誤り訂正した後に、ダウンロードメモリ管理部182に出力する。

【0290】

ステップSR3：ダウンロードメモリ管理部182は、相互認証部170と図63に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304をダウンロードメモリ167に書き込む。

【0291】

ステップSR4：ダウンロードメモリ管理部182は、相互認証部170と図63に示すメディアSAM167aとの間で相互認証を行なった後に、セキュアコンテナ304に格納された図53 (B) に示すキーファイルKFを読み出してセキュアコンテナ復号部183に出力する。

そして、セキュアコンテナ復号部183は、記憶部192から入力した対応する期間の配信用鍵データ $KD_1 \sim KD_3$ を用いて、キーファイルKFを復号する。

【0292】

ステップSR5：セキュアコンテナ復号部183は、図53 (B) に示す署名・証明書モジュール Mod_1 に格納された署名データ $SIG_{1,ESC}$ 、 $SIG_{2,cp} \sim SIG_{4,cp}$ を署名処理部589に出力する。

署名処理部589は、図53 (B) に示す署名データ $SIG_{1,ESC}$ の検証を行なった後に、公開鍵証明書データ CER_{cp} 内に格納された公開鍵データ $K_{CP,P}$ を用いて署名データ $SIG_{2,cp} \sim SIG_{4,cp}$ の検証を行なう。

【0293】

ステップSR6：セキュアコンテナ復号部183は、署名データ $SIG_{2,cp} \sim$

SIG_{4,cp}の正当性が確認されると、キーファイルKFをスタックメモリ200に書き込む。

【0294】

以下、サービスプロバイダ310からダウンロードメモリ167にダウンロードされたセキュアコンテナ304の購入形態を決定するまでの処理の流れを図67および図69を参照しながら説明する。

図69は、当該処理のフローチャートである。

ステップSS1：課金処理部587において、ユーザによる図63に示す購入・利用形態決定操作部165の操作によって、試聴モードを示す操作信号S165が入力されたか否かが判断され、入力されたと判断された場合にはステップSS2の処理が実行され、そうでない場合にはステップSS3の処理が実行される。

【0295】

ステップSS2：例えば、ダウンロードメモリ167に記憶されているコンテンツファイルCFが、復号・伸長モジュール管理部184を介して、図63に示す復号・伸長モジュール163に出力される。

このとき、コンテンツファイルCFに対して、相互認証部170とメディアSAM167aとの間の相互認証およびセッション鍵データK_{SES}による暗号化・復号と、相互認証部170と相互認証部220との間の相互認証およびセッション鍵データK_{SES}による暗号化・復号とが行なわれる。

コンテンツファイルCFは、図63に示す復号部221において復号された後に、復号部222に出力される。

【0296】

また、スタックメモリ200から読み出されたコンテンツ鍵データK_cおよび半開示パラメータデータ199が、図63に示す復号・伸長モジュール163に出力される。このとき、相互認証部170と相互認証部220との間の相互認証後に、コンテンツ鍵データK_cおよび半開示パラメータデータ199に対してセッション鍵データK_{SES}による暗号化および復号が行なわれる。

次に、復号された半開示パラメータデータ199が半開示処理部225に出力

され、半開示処理部225からの制御によって、復号部222によるコンテンツ鍵データ K_c を用いたコンテンツデータCの復号が半開示で行われる。

次に、半開示で復号されたコンテンツデータCが、伸長部223において伸長された後に、電子透かし情報処理部224に出力される。

次に、電子透かし情報処理部224においてユーザ電子透かし情報用データ196がコンテンツデータCに埋め込まれた後、コンテンツデータCが再生モジュール169において再生され、コンテンツデータCに応じた音響が出力される。

【0297】

ステップSS3：コンテンツを試聴したユーザが、購入・利用形態決定操作部165を操作して購入形態を決定すると、当該決定した購入形態を示す操作信号S165が課金処理部187に出力される。

【0298】

ステップSS4：課金処理部187において、決定された購入形態に応じた利用履歴データ308および利用制御状態データ166が生成され、利用履歴データ308が外部メモリ管理部811を介して外部メモリ201に書き込まれると共に利用制御状態データ166がスタックメモリ200に書き込まれる。

以後は、利用監視部186において、利用制御状態データ166によって許諾された範囲で、コンテンツの購入および利用が行なわれるように制御（監視）される。

【0299】

ステップSS5：スタックメモリ200に格納されているキーファイル K_F に、利用制御状態データ166が加えられ、購入形態が決定した後述する図71に示す新たなキーファイル $K_{F_{11}}$ が生成される。キーファイル $K_{F_{11}}$ は、スタックメモリ200に記憶される。

図71に示すように、キーファイル K_{F_1} に格納された利用制御状態データ166はストレージ鍵データ K_{STR} を用いてDESのCBCモードを利用して暗号化されている。また、当該ストレージ鍵データ K_{STR} をMAC鍵データとして用いて生成したMAC値である MAC_{300} が付されている。また、利用制御状態データ166および MAC_{300} からなるモジュールは、メディア鍵データ MED を用

いてDESのCBCモードを利用して暗号化されている。また、当該モジュールには、当該メディア鍵データ K_{MED} をMAC鍵データとして用いて生成したMAC値である MAC_{301} が付されている。

【0300】

次に、ダウンロードメモリ167に記憶されている購入形態が既に決定されたコンテンツデータCを再生する場合の処理の流れを、図67および図70を参照しながら説明する。

図70は、当該処理のフローチャートである。

ステップST1：例えば、ユーザによる操作に応じて、再生対象となるコンテンツの指定をSAMが受ける。

【0301】

ステップST2：利用監視部186の監視下で、操作信号S165に基づいて、ダウンロードメモリ167に記憶されているコンテンツファイルCFが読み出される。

ステップST3：当該読み出されたコンテンツファイルCFが、図63に示す復号・伸長モジュール163に出力される。

また、スタックメモリ200から読み出されたコンテンツ鍵データ K_c が復号・伸長モジュール163に出力される。

【0302】

ステップST4：復号・伸長モジュール163の復号部222において、コンテンツ鍵データ K_c を用いたコンテンツファイルCFの復号と、伸長部223による伸長処理とが行なわれ、再生モジュール169において、コンテンツデータCが再生される。

ステップST5：課金処理部587において、操作信号S165に応じて、利用履歴データ308が更新される。

利用履歴データ308は、秘密鍵データ $K_{SAM1,S}$ を用いて作成したそれぞれ署名データ $SIG_{205,SAM1}$ と共に、EMDサービスセンタ管理部185を介して、所定のタイミングで、EMDサービスセンタ302に送信される。

【0303】

以下、図72に示すように、例えば、ネットワーク機器360₁のダウンロードメモリ167にダウンロードされた既に購入形態が決定されたコンテンツファイルCFを、バス191を介して、AV機器360₂のSAM305₂に転送する場合のSAM305₁内での処理の流れを図73および図74を参照しながら説明する。

ステップSU1：ユーザは、購入・利用形態決定操作部165を操作して、ダウンロードメモリ167に記憶された所定のコンテンツをAV機器360₂に転送することを指示し、当該操作に応じた操作信号S165が、課金処理部587に出力される。

これにより、課金処理部587は、操作信号S165に基づいて、スタックメモリ200に記憶されている利用履歴データ308を更新する。

【0304】

ステップSU2：ダウンロードメモリ管理部182は、ダウンロードメモリ167から読み出した図75（A）に示すコンテンツファイルCFをSAM管理部190に出力する。

ステップSU3：スタックメモリ200から読み出した図75（B）に示す既に購入形態が決定されたキーファイルKF₁₁を、署名処理部589およびSAM管理部190に出力する。

ステップSU4：署名処理部589は、キーファイルKF₁₁の署名データSIG_{80,SAM1}を作成し、これをSAM管理部190に出力する。

【0305】

ステップSU5：SAM管理部190は、記憶部192から、図75（C）に示す公開鍵証明書データCER_{SAM1}およびその署名データSIG_{22,ESC}を読み出す。

また、相互認証部170は、SAM305₂との間で相互認証を行って得たセッション鍵データK_{SES}を暗号化・復号部171に出力する。

SAM管理部190は、図75（A），（B），（C）に示すデータからなるセキュアコンテナを作成する。

【0306】

ステップSU6：暗号化・復号部171において、セッション鍵データ K_{SES} を用いて当該セキュアコンテナを暗号化して作成して、図73に示すAV機器360₂のSAM305₂に出力する。

【0307】

以下、図72に示すように、SAM305₁から入力したコンテンツファイルCFなどを、RAM型などの記録媒体（メディア）に書き込む際のSAM305₂内での処理の流れを、図76および図77を参照しながら説明する。

図77は、当該処理のフローチャートである。

【0308】

ステップSV1：SAM305₂のSAM管理部190は、図76に示すように、図75（A）に示すコンテンツファイルCF、図75（B）に示すキーファイル KF_{11} およびその署名データ $SIG_{80,SAM1}$ と、図75（C）に示す公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22,ESC}$ とを、ネットワーク機器360₁のSAM305₁から入力する。

そして、暗号化・復号部171において、SAM管理部190が入力したコンテンツファイルCFと、キーファイル KF_{11} およびその署名データ $SIG_{80,SAM1}$ と、公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22,ESC}$ とが、相互認証部170とSAM305₁の相互認証部170との間の相互認証によって得られたセッション鍵データ K_{SES} を用いて復号される。

【0309】

次に、セッション鍵データ K_{SES} を用いて復号されたコンテンツファイルCFがメディアSAM管理部197に出力される。

また、セッション鍵データ K_{SES} を用いて復号されたキーファイル KF_{11} およびその署名データ $SIG_{80,SAM1}$ と、公開鍵署名データ CER_{SAM1} およびその署名データ $SIG_{22,ESC}$ とが、スタックメモリ200に書き込まれる。

【0310】

ステップSV2：署名処理部589は、スタックメモリ200から読み出した署名データ $SIG_{22,ESC}$ を、記憶部192から読み出した公開鍵データ $K_{ESC,P}$

を用いて検証して、公開鍵証明書データ CER_{SAM1} の正当性を確認する。

そして、署名処理部 589 は、公開鍵証明書データ CER_{SAM1} の正当性を確認すると、公開鍵証明書データ CER_{SAM1} に格納された公開鍵データ $K_{SAM1,P}$ を用いて、署名データ $SIG_{80,SAM1}$ の正当性を確認する。

【0311】

ステップSV3：署名データ $SIG_{80,SAM1}$ の正当性を確認されると、図75 (B) に示すキーファイル KF_{11} をスタックメモリ200から読み出して暗号化・復号部173に出力する。

そして、暗号化・復号部173は、記憶部192から読み出した記録用鍵データ K_{STR} 、メディア鍵データ K_{MED} および購入者鍵データ K_{PIN} を用いてキーファイル KF_{11} を順に暗号化してメディアSAM管理部197に出力する。

【0312】

ステップSV4：メディアSAM管理部197は、SAM管理部190から入力したコンテンツファイルCFおよび暗号化・復号部173から入力したキーファイル KF_{11} を、図72に示す記録モジュール260に出力する。

そして、記録モジュール260は、メディアSAM管理部197から入力したコンテンツファイルCFおよびキーファイル KF_{11} を、図72に示すRAM型の記録媒体250のRAM領域251に書き込む。

【0313】

なお、 $SAM305_1$ 内での処理のうち、コンテンツの購入形態が未決定のROM型の記録媒体の購入形態を決定する際のAV機器360₂ 内での処理の流れ、AV機器360₃ において購入形態が未決定のROM型の記録媒体からセキュアコンテナ304を読み出してこれをAV機器360₂ に転送してRAM型の記録媒体に書き込む際の処理の流れは、サービスプロバイダ310の秘密鍵データを用いた署名データの署名データの検証を行なう点と、購入形態を決定したキーファイル内にプライスタグデータ312を格納する点を除いて、第1実施形態の $SAM105_1$ の場合と同じである。

【0314】

次に、図49に示すEMDシステム300の全体動作について説明する。

図78および図79は、EMDシステム300の全体動作のフローチャートである。

ここでは、サービスプロバイダ310からユーザホームネットワーク303にオンラインでセキュアコンテナ304を送信する場合を例示して説明する。

なお、以下に示す処理の前提として、EMDサービスセンタ302へのコンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄の登録は既に終了しているものとする。

【0315】

ステップS21：EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データ $K_{CP,P}$ の公開鍵証明書 CER_{CP} を、自らの署名データ SIG_1, ESC と共にコンテンツプロバイダ301に送信する。

また、EMDサービスセンタ302は、コンテンツプロバイダ301の公開鍵データ $K_{SP,P}$ の公開鍵証明書 CER_{SP} を、自らの署名データ $SIG_{61,ESC}$ と共にサービスプロバイダ310に送信する。

また、EMDサービスセンタ302は、各々有効期限が1カ月の6カ月分の配信用鍵データ $KD_1 \sim KD_6$ をコンテンツプロバイダ301に送信し、3カ月分の配信用鍵データ $KD_1 \sim KD_3$ をユーザホームネットワーク303のSAM305₁～305₄に送信する。

【0316】

ステップS22：コンテンツプロバイダ301は、図7(A)に示す権利登録要求モジュール Mod_2 を、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ302は、所定の署名検証を行った後に、権利書データ106およびコンテンツ鍵データ K_c を登録して権威化（認証）する。

【0317】

ステップS23：コンテンツプロバイダ301は、署名データの作成処理や、 SIG 対応する期間の配信用鍵データ $KD_1 \sim KD_3$ などを用いた暗号化処理を経て、図4(A)，(B)，(C)に示すデータを格納したセキュアコンテナ104を、サービスプロバイダ310に供給する。

【0318】

ステップS24：サービスプロバイダ310は、図4（C）に示す署名データ $SIG_{1,ESC}$ を検証した後に、公開鍵証明書データ CER_{CP} に格納された公開鍵データ $K_{CP,P}$ を用いて、図4（A），（B）に示す署名データ $SIG_{6,CP}$ および $SIG_{7,CP}$ を検証して、セキュアコンテナ104が正当なコンテンツプロバイダ301から送信されたものであるかを確認する。

【0319】

ステップS25：サービスプロバイダ310は、プライスタグデータ312を作成し、プライスタグデータ312を格納した図53に示すセキュアコンテナ304を作成する。

【0320】

ステップS26：サービスプロバイダ310は、図55に示すプライスタグ登録要求モジュール Mod_{102} を、EMDサービスセンタ302に送信する。

そして、EMDサービスセンタ302は、所定の署名検証を行った後に、プライスタグデータ312を登録して権威化する。

【0321】

ステップS27：サービスプロバイダ310は、例えば、ユーザホームネットワーク303のCAモジュール311からの要求に応じて、ステップS25で作成したセキュアコンテナ304を、オンラインあるいはオフラインで、図63に示すネットワーク機器360₁の復号モジュール905に送信する。

【0322】

ステップS28：CAモジュール311は、SP用購入履歴データ309を作成し、これを所定のタイミングで、サービスプロバイダ310に送信する。

【0323】

ステップS29： $SAM_{305_1} \sim 305_4$ のいずれかにおいて、図53（D）に示す署名データ $SIG_{61,ESC}$ を検証した後に、公開鍵証明書データ CER_{SP} に格納された公開鍵データ $K_{SP,P}$ を用いて、図53（A），（B），（C）に示す署名データ $SIG_{62,SP}$ 、 $SIG_{63,SP}$ 、 $SIG_{64,SP}$ を検証して、セキュアコンテナ304が正当なサービスプロバイダ310から送信されたものであるか

を確認する。

【0324】

ステップS30: SAM305₁ ~ 305₄ のいずれかにおいて、配信用鍵データKD₁ ~ KD₃ を用いて、図53 (B) に示すキーファイルKFを復号する。そして、SAM305₁ ~ 305₄ のいずれかにおいて、図53 (B) に示す署名データSIG_{1,ESC} を検証した後に、公開鍵証明書データCER_{CP}に格納された公開鍵データK_{CP,P}を用いて、図53 (B) に示す署名データSIG_{2,CP}、SIG_{3,CP}およびSIG_{4,CP}を検証して、コンテンツデータC、コンテンツ鍵データK_cおよび権利書データ106が正当なコンテンツプロバイダ301によって作成されたものであるかを確認する。

【0325】

ステップS31: ユーザが図63の購入・利用形態決定操作部165を操作してコンテンツの購入・利用形態を決定する。

【0326】

ステップS32: ステップS31において生成された操作信号S165に基づいて、SAM305₁ ~ 305₄ において、セキュアコンテナ304の利用履歴(Usage Log) データ308が生成される。

SAM305₁ ~ 305₄ からEMDサービスセンタ302に、利用履歴データ308およびその署名データSIG_{205,SAM1}が送信される。

【0327】

EMDサービスセンタ302は、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310の各々について、課金内容を決定(計算)し、その結果に基づいて、決済請求権データ152_c、152_sを作成する。

【0328】

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152_c、152_sを自らの署名データと共に送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310の

所有者に分配される。

【0329】

以上説明したように、EMDシステム300では、図4に示すフォーマットのセキュアコンテナ104をコンテンツプロバイダ301からサービスプロバイダ310に配給し、セキュアコンテナ104内のコンテンツファイルCFおよびキーファイルKFをそのまま格納したセキュアコンテナ304をサービスプロバイダ310からユーザホームネットワーク303に配給し、キーファイルKFについての処理をSAM305₁～305₄内で行う。

また、キーファイルKFに格納されたコンテンツ鍵データKcおよび権利書データ106は、配信鍵データKD₁～KD₃を用いて暗号化されており、配信鍵データKD₁～KD₃を保持しているSAM305₁～305₄内でのみ復号される。そして、SAM305₁～305₄では、耐タンパ性を有するモジュールであり、権利書データ106に記述されたコンテンツデータCの取り扱い内容に基づいて、コンテンツデータCの購入形態および利用形態が決定される。

【0330】

従って、EMDシステム300によれば、ユーザホームネットワーク303におけるコンテンツデータCの購入および利用を、サービスプロバイダ310における処理とは無関係に、コンテンツプロバイダ101の関係者が作成した権利書データ106の内容に基づいて確実に行わせることができる。すなわち、EMDシステム300にれば、権利書データ106をサービスプロバイダ310が管理できないようできる。

そのため、EMDシステム300によれば、異系列の複数のサービスプロバイダ310を介してユーザホームネットワーク303にコンテンツデータCが配給された場合でも、ユーザホームネットワーク303における当該コンテンツデータCについての権利処理を、コンテンツプロバイダ301が作成した共通の権利書データ106に基づいて行わせることができる。

【0331】

また、EMDシステム300では、サービスプロバイダ310からユーザホームネットワーク103へのコンテンツデータCの配給を、オンラインおよびオフ

ラインの何れの場合でもセキュアコンテナ304を用いて行うことで、双方の場合において、SAM305₁～305₄におけるコンテンツデータCの権利処理を共通化できる。

【0332】

また、EMDシステム300では、ユーザホームネットワーク303内のネットワーク機器360₁ およびAV機器360₂～360₄においてコンテンツデータCを購入、利用、記録および転送する際に、常に権利書データ106に基づいて処理を行うことで、共通の権利処理ルールを採用できる。

【0333】

また、EMDシステム300によれば、EMDサービスセンタ302が、認証機能、鍵データ管理機能および権利処理（利益分配）機能を有することから、コンテンツの利用に伴ってユーザが支払った金額が、コンテンツプロバイダ301およびEMDサービスセンタ302の所有者に、予め決められた比率に従って確実に分配される。

また、EMDシステム300によれば、同じコンテンツプロバイダ301が供給した同じコンテンツファイルCFについての権利書データ106は、サービスプロバイダ310のサービス形態とは無関係に、そのままSAM305₁～305₄に供給される。従って、SAM305₁～305₄において、権利書データ106に基づいて、コンテンツプロバイダ301の意向通りに、コンテンツファイルCFの利用を行わせることができる。

すなわち、EMDシステム300によれば、コンテンツを用いたサービスおよびユーザによるコンテンツの利用が行われる際に、従来のように監査組織725に頼ることなく、技術的な手段によって、コンテンツプロバイダ301の所有者の権利および利益を確実に守ることができる。

【0334】

第2実施形態の第1変形例

図80は、第2実施形態の第1変形例に係わる2個のサービスプロバイダを用いたEMDシステム300aの構成図である。

図80において、図49と同一符号を付した構成要素は、第2実施形態で説明

した同一符号の構成要素と同じである。

図80に示すように、EMDシステム300aでは、コンテンツプロバイダ301からサービスプロバイダ310aおよび310bに、同じセキュアコンテナ104を供給する。

【0335】

サービスプロバイダ310aは、例えば、コンテンツをドラマ番組の提供サービスを行っており、当該サービスにおいて、当該ドラマ番組に関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312aとを格納したセキュアコンテナ304aを作成し、これをネットワーク機器360₁に配給する。

また、サービスプロバイダ310bは、例えば、カラオケサービスを提供しており、当該サービスにおいて、当該カラオケサービスに関連するコンテンツデータCと、当該コンテンツデータCについて独自に作成したプライスタグデータ312bとを格納したセキュアコンテナ304bを作成し、これをネットワーク機器360₁に配給する。

ここで、セキュアコンテナ304a、304bのフォーマットは、図53を用いた説明したセキュアコンテナ304と同じである。

【0336】

ネットワーク機器360a₁には、サービスプロバイダ310a、310bの各々に対応したCAモジュール311a、311bが設けられている。

CAモジュール311a、311bは、自らの要求に応じたセキュアコンテナ304a、304bの配給を、それぞれサービスプロバイダ310a、310bから受ける。

【0337】

次に、CAモジュール311a、311bは、配給されたセキュアコンテナ304a、304bに応じたSP用購入履歴データ309a、309bをそれぞれ作成し、これらをそれぞれサービスプロバイダ310a、310bに送信する。

また、CAモジュール311a、311bは、セキュアコンテナ304a、304bをセッション鍵データK_{SES}で復号した後に、SAM305₁～305₄

に出力する。

【0338】

次に、SAM305₁～305₄において、共通の配信用鍵データKD₁～KD₃を用いて、セキュアコンテナ304a, 304b内のキーファイルKFが復号され、共通の権利書データ106に基づいて、ユーザからの操作に応じたコンテンツの購入・利用に関する処理が行われ、それに応じた利用履歴データ308が作成される。

【0339】

そして、SAM305₁～305₄からEMDサービスセンタ302に、利用履歴データ308が送信される。

【0340】

EMDサービスセンタ302では、利用履歴データ308に基づいて、コンテンツプロバイダ301およびサービスプロバイダ310a, 310bの各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ152c, 152sa, 152sbを作成する。

【0341】

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152c, 152sa, 152sbを送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301およびサービスプロバイダ310a, 310bの所有者に分配される。

【0342】

上述したように、EMDシステム300bによれば、同じコンテンツファイルCFをサービスプロバイダに310a, 310bに供給する場合に、当該コンテンツファイルCFについての権利書データ106を配信用鍵データKD₁～KD₆で暗号化してサービスプロバイダに310a, 310bに供給し、サービスプロバイダに310a, 310bは暗号化された権利書データ106をそのまま格納したセキュアコンテナ304a, 304bをユーザホームネットワークに配給する。そのため、ユーザホームネットワーク内のSAM305₁～305₄では

、コンテンツファイルCFをサービスプロバイダに310a, 310bの何れから配給を受けた場合でも、共通の権利書データ106に基づいて権利処理を行うことができる。

【0343】

なお、上述した第1変形例では、2個のサービスプロバイダを用いた場合を例示したが、本発明では、サービスプロバイダの数は任意である。

【0344】

第2実施形態の第2変形例

図81は、第2実施形態の第2変形例に係わる複数のコンテンツプロバイダを用いたEMDシステム300bの構成図である。

図81において、図49と同一符号を付した構成要素は、第2実施形態で説明した同一符号の構成要素と同じである。

図81に示すように、EMDシステム300bでは、コンテンツプロバイダ301a, 301bからサービスプロバイダ310に、それぞれセキュアコンテナ104a, 104bが供給される。

【0345】

サービスプロバイダ310は、例えば、コンテンツプロバイダ301a, 301bが供給したコンテンツを用いてサービスを提供しており、セキュアコンテナ104aについてのプライスタグデータ312aと、セキュアコンテナ104bについてのプライスタグデータ312bとをそれぞれ生成し、これらを格納したセキュアコンテナ304cを作成する。

図81に示すように、セキュアコンテナ304cには、コンテンツファイルCFa, CFb、キーファイルKF a, KF b、プライスタグデータ312a, 312b、それらの各々についてのサービスプロバイダ310の秘密鍵データ $K_{CP,s}$ による署名データが格納されている。

【0346】

セキュアコンテナ304cは、ユーザホームネットワーク303のネットワーク機器360₁のCAモジュール311で受信された後に、SAM305₁～305₄において処理される。

【0347】

SAM305₁ ~ 305₄ では、配信用鍵データKD a₁ ~ KD a₃ を用いて、キーファイルKF aが復号され、権利書データ106 aに基づいて、コンテンツファイルCF aについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ308に記述される。

また、SAM305₁ ~ 305₄ において、配信用鍵データKD b₁ ~ KD b₃ を用いて、キーファイルKF bが復号され、権利書データ106 bに基づいて、コンテンツファイルCF bについてのユーザからの操作に応じた購入・利用に関する処理が行われ、その履歴が利用履歴データ308に記述される。

【0348】

そして、SAM305₁ ~ 305₄ からEMDサービスセンタ302に、利用履歴データ308が送信される。

【0349】

EMDサービスセンタ302では、利用履歴データ308に基づいて、コンテンツプロバイダ301 a, 301 bおよびサービスプロバイダ310の各々について、課金内容を決定（計算）し、その結果に基づいて、それぞれに対応する決済請求権データ152 c a, 152 c b, 152 sを作成する。

【0350】

EMDサービスセンタ302は、ペイメントゲートウェイ90を介して決済機関91に、決済請求権データ152 c a, 152 c b, 152 sを送信し、これにより、ユーザホームネットワーク303のユーザが決済機関91に支払った金銭が、コンテンツプロバイダ301 a, 301 bおよびサービスプロバイダ310の所有者に分配される。

【0351】

上述したように、EMDシステム300 bによれば、セキュアコンテナ304 c内に格納されたコンテンツファイルCF a, CF bの権利書データ106 a, 106 bは、コンテンツプロバイダ301 a, 301 bが作成したものをそのまま用いるため、SAM305₁ ~ 305₄ 内において、権利書データ106 a, 106 bに基づいて、コンテンツファイルCF a, CF bについての権利処理が

コンテンツプロバイダ 3 0 1 a, 3 0 1 b の意向に沿って確実に行われる。

【0 3 5 2】

なお、図 8 1 に示す第 2 変形例では、2 個のコンテンツプロバイダを用いた場合を例示したが、コンテンツプロバイダの数は任意である。

また、コンテンツプロバイダおよびサービスプロバイダの双方が複数であってもよい。

【0 3 5 3】

第 2 実施形態の第 3 変形例

図 8 2 は、第 2 実施形態の第 3 変形例に係わる EMD システムの構成図である。

上述した第 2 実施形態では、EMD サービスセンタ 3 0 2 が決済機関 9 1 に対して、コンテンツプロバイダ 3 0 1 およびサービスプロバイダ 3 1 0 の決済を行う場合を例示したが、本発明では、例えば、図 8 2 に示すように、EMD サービスセンタ 3 0 2 において、利用履歴データ 3 0 8 に基づいて、コンテンツプロバイダ 3 0 1 のための決済請求権データ 1 5 2 c と、サービスプロバイダ 3 1 0 のための決済請求権データ 1 5 2 s とを作成し、これらをそれぞれコンテンツプロバイダ 3 0 1 およびサービスプロバイダ 3 1 0 に送信するようにしてもよい。

この場合には、コンテンツプロバイダ 3 0 1 は、決済請求権データ 1 5 2 c を用いて、ペイメントゲートウェイ 9 0 a を介して決済機関 9 1 a に決済を行う。また、サービスプロバイダ 3 1 0 は、決済請求権データ 1 5 2 s を用いて、ペイメントゲートウェイ 9 0 b を介して決済機関 9 1 b に決済を行う。

【0 3 5 4】

第 2 実施形態の第 4 変形例

図 8 3 は、第 2 実施形態の第 4 変形例に係わる EMD システムの構成図である。

上述した第 2 実施形態では、例えば現行のインターネットのようにサービスプロバイダ 3 1 0 が課金機能を有していない場合を例示したが、現行のデジタル放送などのようにサービスプロバイダ 3 1 0 が課金機能を有している場合には、C A モジュール 3 1 1 において、セキュアコンテナ 3 0 4 に関するサービスプロバ

イダ310のサービスに対しての利用履歴データ308sを作成してサービスプロバイダ310に送信する。

そして、サービスプロバイダ310は、利用履歴データ308sに基づいて、課金処理を行って決済請求権データ152sを作成し、これを用いてペイメントゲートウェイ90bを介して決済機関91bに決済を行う。

一方、SAM305₁～305₄は、セキュアコンテナ304に関するコンテンツプロバイダ301の権利処理に対しての利用履歴データ308cを作成し、これをEMDサービスセンタ302に送信する。

EMDサービスセンタ302は、利用履歴データ308cに基づいて、決済請求権データ152cを作成し、これをコンテンツプロバイダ301に送信する。

コンテンツプロバイダ301は、決済請求権データ152cを用いて、ペイメントゲートウェイ90aを介して決済機関91aに決済を行う。

【0355】

第2実施形態の第5変形例

上述した実施形態では、図49に示すように、EMDサービスセンタ302のユーザ嗜好フィルタ生成部901において、SAM305₁などから受信した利用履歴データ308に基づいて、ユーザ嗜好フィルタデータ903を生成する場合を例示したが、例えば、図67に示すSAM305₁などの利用監視部186で生成した利用制御状態データ166をリアルタイムでEMDサービスセンタ302に送信するようにして、SP用購入履歴データ309において、利用制御状態データ166に基づいてユーザ嗜好フィルタデータ903を生成するようにしてもよい。

【0356】

第2実施形態の第6変形例

コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄は、それぞれ自らの公開鍵データ $K_{CP,P}$ 、 $K_{SP,P}$ 、 $K_{SAM1,P} \sim K_{SAM4,P}$ の他に、自らの秘密鍵データ $K_{CP,S}$ 、 $K_{SP,S}$ 、 $K_{SAM1,S} \sim K_{SAM4,S}$ をEMDサービスセンタ302に登録してもよい。

このようにすることで、EMDサービスセンタ302は、緊急時に、国家ある

いは警察機関などからの要請に応じて、秘密鍵データ $K_{CP,S}$, $K_{SP,S}$, $K_{SAM1,S}$ ~ $K_{SAM4,S}$ を用いて、コンテンツプロバイダ 301 とサービスプロバイダ 310 との間の通信、サービスプロバイダ 310 と $SAM305_1 \sim 305_4$ との間の通信、並びにユーザホームネットワーク 303 内での $SAM305_1 \sim 305_4$ 相互間での通信のうち対象となる通信を盗聴することが可能になる。

また、 $SAM305_1 \sim 305_4$ については、出荷時に、EMD サービスセンタ 302 によって秘密鍵データ $K_{SAM1,S} \sim K_{SAM4,S}$ を生成し、これを $SAM305_1 \sim 305_4$ に格納すると共に EMD サービスセンタ 302 が保持（登録）するようにしてもよい。

【0357】

第2実施形態の第7変形例

上述した実施形態では、コンテンツプロバイダ 301、サービスプロバイダ 310 および $SAM305_1 \sim 305_4$ が、相互に通信を行う場合に、EMD サービスセンタ 302 から事前に公開鍵証明書データ CER_{CP} , CER_{SP} , $CER_{SAM1} \sim CER_{SAM4}$ を取得し、イン・バンド方式で通信先に送信する場合を例示したが、本発明では、通信先への公開鍵証明書データの送信形態として種々の形態を採用できる。

例えば、コンテンツプロバイダ 301、サービスプロバイダ 310 および $SAM305_1 \sim 305_4$ が、相互に通信を行う場合に、EMD サービスセンタ 302 から事前に公開鍵証明書データ CER_{CP} , CER_{SP} , $CER_{SAM1} \sim CER_{SAM4}$ を取得し、当該通信に先立ってアウト・オブ・バンド方式で通信先に送信してもよい。

また、コンテンツプロバイダ 301、サービスプロバイダ 310 および $SAM305_1 \sim 305_4$ が、通信時に、EMD サービスセンタ 302 から公開鍵証明書データ CER_{CP} , CER_{SP} , $CER_{SAM1} \sim CER_{SAM4}$ を取得してもよい。

【0358】

図 84 は、公開鍵証明書データの取得（入手）ルートの形態を説明するための図である。

なお、図 84 において、図 49 と同じ符号を付した構成要素は、前述した同一

符号の構成要素と同じである。また、ユーザホームネットワーク 303a は、前述したユーザホームネットワーク 303 と同じである。ユーザホームネットワーク 303b では、IEEE 1394 シリアルバスであるバス 191 を介して SAM305₁₁ ~ 305₁₄ を接続している。

【0359】

コンテンツプロバイダ 301 がサービスプロバイダ 310 の公開鍵証明書データ CER_{SP} を取得する場合には、例えば、通信に先立ってサービスプロバイダ 310 からコンテンツプロバイダ 301 に公開鍵証明書データ CER_{SP} を送信する場合（図 84 中（3））と、コンテンツプロバイダ 301 が EMD サービスセンタ 302 から公開鍵証明書データ CER_{SP} を取り寄せる場合（図 84 中（1））とがある。

【0360】

また、サービスプロバイダ 310 がコンテンツプロバイダ 301 の公開鍵証明書データ CER_{CP} を取得する場合には、例えば、通信に先立ってコンテンツプロバイダ 301 からサービスプロバイダ 310 に公開鍵証明書データ CER_{CP} を送信する場合（図 84 中（2））と、サービスプロバイダ 310 が EMD サービスセンタ 302 から公開鍵証明書データ CER_{CP} を取り寄せる場合（図 84 中（4））とがある。

【0361】

また、サービスプロバイダ 310 が SAM305₁ ~ 305₄ の公開鍵証明書データ CER_{SAM1} ~ CER_{SAM4} を取得する場合には、例えば、通信に先立って SAM305₁ ~ 305₄ からサービスプロバイダ 310 に公開鍵証明書データ CER_{SAM1} ~ CER_{SAM4} を送信する場合（図 84 中（6））と、サービスプロバイダ 310 が EMD サービスセンタ 302 から公開鍵証明書データ CER_{SAM1} ~ CER_{SAM4} を取り寄せる場合（図 84 中（4））とがある。

【0362】

また、SAM305₁ ~ 305₄ がサービスプロバイダ 310 の公開鍵証明書データ CER_{SP} を取得する場合には、例えば、通信に先立ってサービスプロバイダ 310 から SAM305₁ ~ 305₄ に公開鍵証明書データ CER_{SP} を送信す

る場合 (図84中(5)) と、 $SAM305_1 \sim 305_4$ が EMD サービスセンタ 302 から公開鍵証明書データ CER_{SP} を取り寄せる場合 (図84中(7) など) とがある。

【0363】

また、 $SAM305_1$ が $SAM305_2$ の公開鍵証明書データ CER_{SAM2} を取得する場合には、例えば、通信に先立って $SAM305_2$ から $SAM305_1$ に公開鍵証明書データ CER_{SAM2} を送信する場合 (図84中(8)) と、 $SAM305_1$ が EMD サービスセンタ 302 から公開鍵証明書データ CER_{SAM2} を取り寄せる場合 (図84中(7) など) とがある。

【0364】

また、 $SAM305_2$ が $SAM305_1$ の公開鍵証明書データ CER_{SAM1} を取得する場合には、例えば、通信に先立って $SAM305_1$ から $SAM305_2$ に公開鍵証明書データ CER_{SAM1} を送信する場合 (図84中(9)) と、 $SAM305_2$ が自ら EMD サービスセンタ 302 から公開鍵証明書データ CER_{SAM1} を取り寄せる場合と、 $SAM305_1$ が搭載されたネットワーク機器を介して公開鍵証明書データ CER_{SAM1} を取り寄せる場合 (図84中(7), (8)) とがある。

【0365】

また、 $SAM305_4$ が $SAM305_{13}$ の公開鍵証明書データ CER_{SAM13} を取得する場合には、例えば、通信に先立って $SAM305_{13}$ から $SAM305_4$ に公開鍵証明書データ CER_{SAM13} を送信する場合 (図84中(12)) と、 $SAM305_4$ が自ら EMD サービスセンタ 302 から公開鍵証明書データ CER_{SAM13} を取り寄せる場合 (図84中(10)) と、ユーザホームネットワーク 303b 内のネットワーク機器を介して公開鍵証明書データ CER_{SAM13} を取り寄せる場合とがある。

【0366】

また、 $SAM305_{13}$ が $SAM305_4$ の公開鍵証明書データ CER_{SAM4} を取得する場合には、例えば、通信に先立って $SAM305_4$ から $SAM305_{13}$ に公開鍵証明書データ CER_{SAM4} を送信する場合 (図84中(11)) と、 SAM

305₁₃が自らEMDサービスセンタ302から公開鍵証明書データCER_{SAM4}を取り寄せる場合(図84中(13))と、ユーザホームネットワーク303b内のネットワーク機器を介して公開鍵証明書データCER_{SAM4}を取り寄せる場合とがある。

【0367】

第2実施形態における公開鍵証明書破棄リスト(データ)の取り扱い

第2実施形態では、EMDサービスセンタ302において、不正行為などに用いられたコンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄が他の装置と通信できないようにするために、当該不正行為に用いられた装置の公開鍵証明書データを無効にする公開鍵証明書破棄データを作成する。そして、当該公開鍵証明書破棄データCRL(Certificate Revocation List)を、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄に送信する。

なお、公開鍵証明書破棄データCRLは、EMDサービスセンタ302の他に、例えば、コンテンツプロバイダ301、サービスプロバイダ310およびSAM305₁～305₄において生成してもよい。

【0368】

先ず、EMDサービスセンタ302が、コンテンツプロバイダ301の公開鍵証明書データCER_{CP}を無効にする場合について説明する。

図85に示すように、EMDサービスセンタ302は、公開鍵証明書データCER_{CP}を無効にすることを示す公開鍵証明書破棄データCRL₁をサービスプロバイダ310に送信する(図85中(1))。サービスプロバイダ310は、コンテンツプロバイダ301から入力した署名データを検証する際に、公開鍵証明書破棄データCRL₁を参照して公開鍵証明書データCER_{CP}の有効性を判断し、有効であると判断した場合に公開鍵データK_{CP,P}を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにコンテンツプロバイダ301からのデータを無効にする。なお、データを無効にするのではなく、通信を拒絶するようにしてもよい。

【0369】

また、EMDサービスセンタ302は、公開鍵証明書破棄データ CRL_1 を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えば $SAM305_1$ に送信する（図85中（1），（2））。 $SAM305_1$ は、サービスプロバイダ310から入力したセキュアコンテナ内に格納されたコンテンツプロバイダ301の署名データを検証する際に、公開鍵証明書破棄データ CRL_1 を参照して公開鍵証明書データ CER_{CP} の有効性を判断し、有効であると判断した場合に公開鍵データ $K_{CP,P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

なお、EMDサービスセンタ302は、公開鍵証明書破棄データ CRL_1 を、ユーザホームネットワーク303内のネットワーク機器を介して $SAM305_1$ に直接送信してもよい（図85中（3））。

【0370】

次に、EMDサービスセンタ302が、サービスプロバイダ310の公開鍵証明書データ CER_{SP} を無効にする場合について説明する。

図86に示すように、EMDサービスセンタ302は、公開鍵証明書データ CER_{SP} を無効にすることを示す公開鍵証明書破棄データ CRL_2 をコンテンツプロバイダ301に送信する（図86中（1））。コンテンツプロバイダ301は、サービスプロバイダ310から入力した署名データを検証する際に、公開鍵証明書破棄データ CRL_2 を参照して公開鍵証明書データ CER_{SP} の有効性を判断し、有効であると判断した場合に公開鍵データ $K_{SP,P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずにサービスプロバイダ310からのデータを無効にする。

【0371】

また、EMDサービスセンタ302は、公開鍵証明書破棄データ CRL_2 を、サービスプロバイダ310の流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えば $SAM305_1$ に送信する（図86中（2））。 $SAM305_1$ は、サービスプロバイダ310

から入力したセキュアコンテナ内に格納されたサービスプロバイダ310の署名データを検証する際に、公開鍵証明書破棄データ CRL_2 を参照して公開鍵証明書データ CER_{SP} の有効性を判断し、有効であると判断した場合に公開鍵データ $K_{SP,P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該セキュアコンテナを無効にする。

この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データ CRL_2 の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データ CRL_2 は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。

なお、EMDサービスセンタ302は、公開鍵証明書破棄データ CRL_2 を、ユーザホームネットワーク303内のネットワーク機器を介して $SAM305_1$ に直接送信してもよい(図86中(3))。

【0372】

次に、EMDサービスセンタ302が、例えば $SAM305_2$ の公開鍵証明書データ CER_{SAM2} を無効にする場合について説明する。

図87に示すように、EMDサービスセンタ302は、公開鍵証明書データ CER_{SAM2} を無効にすることを示す公開鍵証明書破棄データ CRL_3 をコンテンツプロバイダ301に送信する(図87中(1))。コンテンツプロバイダ301は、公開鍵証明書破棄データ CRL_3 をサービスプロバイダ310に送信する。サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、ユーザホームネットワーク303内の例えば $SAM305_1$ に公開鍵証明書破棄データ CRL_{SAM1} を送信する(図87中(1))。 $SAM305_1$ は、 $SAM305_2$ から入力したデータに付加された $SAM305_2$ の署名データを検証する際に、公開鍵証明書破棄データ CRL_3 を参照して公開鍵証明書データ CER_{SAM2} の有効性を判断し、有効であると判断した場合に公開鍵データ $K_{SAM2,P}$ を用いた署名検証を行い、無効であると判断した場合に当該署名検証を行わずに当該データを無効にする。

この場合に、サービスプロバイダ310内において、公開鍵証明書破棄データ

CRL₃ の送受信を行うモジュールは、耐タンパ性を有している必要がある。また、サービスプロバイダ310内において、公開鍵証明書破棄データCRL₃は、サービスプロバイダ310の関係者による改竄な困難な領域に格納される必要がある。

【0373】

EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310を介してSAM305₁に送信してもよい(図87中(1)、(2))。

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を、ユーザホームネットワーク303内のネットワーク機器を介してSAM305₁に直接送信してもよい(図87中(3))。

【0374】

また、EMDサービスセンタ302は、例えばSAM305₂の公開鍵証明書データCER_{SAM2}を無効にすることを示す公開鍵証明書破棄データCRL₃を作成し、これを保管する。

また、ユーザホームネットワーク303は、バス191に接続されているSAMのSAM登録リストSRLを作成し、これをEMDサービスセンタ302に送信する(図88中(1))。

EMDサービスセンタ302は、SAM登録リストに示されるSAM305₁~305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM(例えばSAM305₂)を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定して新たなSAM登録リストSRLを作成する。

次に、EMDサービスセンタ302は、当該生成したSAM登録リストSRLをSAM305₁に送信する(図88中(1))。

SAM305₁は、他のSAMと通信を行う際に、SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0375】

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをコンテンツプロバイダ301に送信する（図88中（2））。

コンテンツプロバイダ301は、公開鍵証明書破棄データCRL₃をサービスプロバイダ310に送信する（図88中（2））。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM305₁に送信する（図88中（2））。

SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM（例えばSAM305₂）を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0376】

また、EMDサービスセンタ302は、公開鍵証明書破棄データCRL₃を作成し、これをサービスプロバイダ310に送信する（図88中（3））。

次に、サービスプロバイダ310は、自らの流通資源を利用して放送型あるいはオンデマンド型のいずれか一方で、公開鍵証明書破棄データCRL₃をSAM305₁に送信する（図88中（3））。

SAM305₁は、自らが作成したSAM登録リストに示されるSAM305₁～305₄のうち、公開鍵証明書破棄データCRL₃によって無効にすることが示されているSAM（例えばSAM305₂）を特定し、SAM登録リストSRL内の当該SAMに対応する破棄フラグを無効を示すように設定する。

以後、SAM305₁は、他のSAMと通信を行う際に、当該SAM登録リストSRLの破棄フラグを参照して、署名データの検証の有無および通信を許否するか否かを決定する。

【0377】

EMDサービスセンタ302の役割等

図89は、図49に示すEMDサービスセンタ（クリアリングハウス）302の機能を権利管理用クリアリングハウス950と、電子決済用クリアリングハウス951とに分割した場合のEMDシステムの構成図である。

当該EMDシステムでは、電子決済用クリアリングハウス951において、ユーザホームネットワーク303a、303bのSAMからの利用履歴データ308に基づいて、決済処理（利益分配処理）を行い、コンテンツプロバイダ301およびサービスプロバイダ310の決済請求権データをそれぞれ生成し、ペイメントゲートウェイ90を介して決済機関91において決済を行う。

【0378】

また、権利管理用クリアリングハウス950は、電子決済用クリアリングハウス951からの決済通知に応じたコンテンツプロバイダ301およびサービスプロバイダ310の決済レポートを作成し、それらをコンテンツプロバイダ301およびコンテンツプロバイダ301に送信する。

また、コンテンツプロバイダ301の権利書データ106およびコンテンツ鍵データKcの登録（権威化）などを行う。

なお、図90に示すように、権利管理用クリアリングハウス950と電子決済用クリアリングハウス951とを単体の装置内に収納すると、図49に示すEMDサービスセンタ302となる。

【0379】

また、本発明は、例えば、図91に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス960の機能を設け、権利管理用クリアリングハウス960において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてサービスプロバイダ310の決済請求権データを作成し、これをサービスプロバイダ310に送信してもよい。この場合には、サービスプロバイダ310は、自らの課金システムを電子決済用クリアリングハウス961として利用し、権利管理用クリアリングハウス960からの決済請求権データに基づいて決済を行う。

【0380】

また、本発明は、例えば、図92に示すように、EMDサービスセンタ302に、権利管理用クリアリングハウス970の機能を設け、権利管理用クリアリングハウス970において、権利書データ106の登録などを行うと共に、SAMからの利用履歴データ308に基づいてコンテンツプロバイダ301の決済請求権データを作成し、これをコンテンツプロバイダ301に送信してもよい。この場合には、コンテンツプロバイダ301は、自らの課金システムを電子決済用クリアリングハウス961として利用し、権利管理用クリアリングハウス970からの決済請求権データに基づいて決済を行う。

【0381】

第2実施形態の第8変形例

上述した第2実施形態では、図49に示すEMDシステム300において、コンテンツプロバイダ301からサービスプロバイダ310に図4に示すフォーマットのセキュアコンテナ104を提供し、サービスプロバイダ310からユーザホームネットワーク303に図53に示すフォーマットのセキュアコンテナ304を配給する場合を例示した。

すなわち、上述した第2実施形態では、図4および図53に示すように、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ単数のコンテンツファイルCFと、当該コンテンツファイルCFに対応する単数のキーファイルKFを格納した場合を例示した。

本発明では、セキュアコンテナ104およびセキュアコンテナ304内に、それぞれ複数のコンテンツファイルCFと、当該複数のコンテンツファイルCFにそれぞれ対応する複数のキーファイルKFとを格納してもよい。

【0382】

図93は、本変形例において、図49に示すコンテンツプロバイダ301からサービスプロバイダ310に提供されるセキュアコンテナ104aのフォーマットを説明するための図である。

図93に示すように、セキュアコンテナ104aには、コンテンツファイルCF₁₀₁、CF₁₀₂、CF₁₀₃、キーファイルKF₁₀₁、KF₁₀₂、KF₁₀₃、公

開鍵証明書データ CER_{CP} 、署名データ $SIG_{1,ESC}$ および署名データ $SIG_{250,CP}$ が格納されている。

ここで、署名データ $SIG_{250,CP}$ は、コンテンツプロバイダ 301 において、コンテンツファイル CF_{101} 、 CF_{102} 、 CF_{103} 、キーファイル KF_{101} 、 KF_{102} 、 KF_{103} 、公開鍵証明書データ CER_{CP} および署名データ $SIG_{1,ESC}$ の全体に対してハッシュ値をとり、コンテンツプロバイダ 301 の秘密鍵データ $K_{cp,s}$ を用いて生成される。

【0383】

コンテンツファイル CF_{101} には、ヘッダ、リンクデータ LD_1 、メタデータ $Meta_1$ 、コンテンツデータ C_1 および A/V 伸長用ソフトウェア $Soft_1$ が格納されている。

ここで、コンテンツデータ C_1 および A/V 伸長用ソフトウェア $Soft_1$ は、前述したコンテンツ鍵データ Kc_1 を用いて暗号化されており、メタデータ $Meta_1$ は必要に応じてコンテンツ鍵データ Kc_1 を用いて暗号化されている。

また、コンテンツデータ C_1 は、例えば、ATRAC3 方式で圧縮されている。A/V 伸長用ソフトウェア $Soft_1$ は、ATRAC3 方式の伸長用のソフトウェアである。

また、リンクデータ LD_1 は、キーファイル KF_{101} にリンクすることを示している。

【0384】

コンテンツファイル CF_{102} には、ヘッダ、リンクデータ LD_1 、メタデータ $Meta_2$ 、コンテンツデータ C_2 および A/V 伸長用ソフトウェア $Soft_2$ が格納されている。

ここで、コンテンツデータ C_2 および A/V 伸長用ソフトウェア $Soft_2$ は、前述したコンテンツ鍵データ Kc_2 を用いて暗号化されており、メタデータ $Meta_2$ は必要に応じてコンテンツ鍵データ Kc_2 を用いて暗号化されている。

また、コンテンツデータ C_2 は、例えば、MPEG2 方式で圧縮されている。
A/V 伸長用ソフトウェア $Soft_2$ は、MPEG2 方式の伸長用のソフトウェアである。

また、リンクデータ LD_2 は、キーファイル KF_{102} にリンクすることを示している。

【0385】

コンテンツファイル CF_{103} には、ヘッダ、リンクデータ LD_3 、メタデータ $Meta_3$ 、コンテンツデータ C_3 および A/V 伸長用ソフトウェア $Soft_3$ が格納されている。

ここで、コンテンツデータ C_3 および A/V 伸長用ソフトウェア $Soft_3$ は、前述したコンテンツ鍵データ Kc_3 を用いて暗号化されており、メタデータ $Meta_3$ は必要に応じてコンテンツ鍵データ Kc_3 を用いて暗号化されている。

また、コンテンツデータ C_3 は、例えば、JPEG 方式で圧縮されている。A/V 伸長用ソフトウェア $Soft_3$ は、JPEG 方式の伸長用のソフトウェアである。

また、リンクデータ LD_3 は、キーファイル KF_{103} にリンクすることを示している。

【0386】

キーファイル KF_{101} には、ヘッダと、それぞれ配信鍵データ $KD_1 \sim KD_3$ を用いて暗号化されたコンテンツ鍵データ Kc_1 、権利書データ 106_1 、SAM プログラム・ダウンロード・コンテナ SDC_1 および署名・証明書モジュール Mod_{200} とが格納されている。

ここで、署名・証明書モジュール Mod_{200} には、図 94 (A) に示すように、それぞれコンテンツデータ C_1 、コンテンツ鍵データ Kc_1 および権利書データ 106_1 のハッシュ値をとり、コンテンツプロバイダ 301 の秘密鍵データ $K_{CP,S}$ を用いて作成した署名データ $SIG_{211,CP}$ 、 $SIG_{212,CP}$ 、 $SIG_{213,CP}$ と、公開鍵データ $K_{CP,P}$ の公開鍵証明書データ CER_{CP} と、当該公開鍵証明書データ CER_{CP} に対しての EMD サービスセンタ 302 の署名データ $SIG_{1,ESC}$ とが格納されている。

【0387】

キーファイル KF_{102} には、ヘッダと、それぞれ配信鍵データ $KD_1 \sim KD_3$ を用いて暗号化されたコンテンツ鍵データ Kc_2 、権利書データ 106_2 、SA

Mプログラム・ダウンロード・コンテナSDC₂ および署名・証明書モジュールMod₂₀₁ とが格納されている。

ここで、署名・証明書モジュールMod₂₀₁ には、図94 (B) に示すように、それぞれコンテンツデータC₂、コンテンツ鍵データKc₂ および権利書データ106₂ のハッシュ値をとり、コンテンツプロバイダ301の秘密鍵データK_{CP,S}を用いて作成した署名データSIG_{221,CP}、SIG_{222,CP}、SIG_{223,CP}と、公開鍵証明書データCER_{CP}と、当該公開鍵証明書データCER_{CP}に対しての署名データSIG_{1,ESC} とが格納されている。

【0388】

キーファイルKF₁₀₃ には、ヘッダと、それぞれ配信鍵データKD₁ ~ KD₃ を用いて暗号化されたコンテンツ鍵データKc₃、権利書データ106₃、SAMプログラム・ダウンロード・コンテナSDC₃ および署名・証明書モジュールMod₂₀₂ とが格納されている。

ここで、署名・証明書モジュールMod₂₀₂ には、図94 (C) に示すように、それぞれコンテンツデータC₃、コンテンツ鍵データKc₃ および権利書データ106₃ のハッシュ値をとり、コンテンツプロバイダ301の秘密鍵データK_{CP,S}を用いて作成した署名データSIG_{231,CP}、SIG_{232,CP}、SIG_{233,CP}と、公開鍵証明書データCER_{CP}と、当該公開鍵証明書データCER_{CP}に対しての署名データSIG_{1,ESC} とが格納されている。

【0389】

サービスプロバイダ310は、図93に示すセキュアコンテナ104aの配給を受けると、EMDサービスセンタ302の公開鍵データK_{ESC,P}を用いて公開鍵証明書データCER_{cp}の正当性を確認した後に、当該公開鍵証明書データCER_{CP}に格納された公開鍵データK_{cp,P}を用いて、署名データSIG_{250,CP}の正当性を確認する。

そして、サービスプロバイダ310は、署名データSIG_{250,CP}の正当性を確認すると、図95に示すように、セキュアコンテナ104aから得たコンテンツファイルCF₁₀₁、CF₁₀₂、CF₁₀₃ およびキーファイルKF₁₀₁、KF₁₀₂、KF₁₀₃ と、サービスプロバイダ310の公開鍵証明書データCER_{SP}と、署

名データ $SIG_{61,ESC}$ と、プライスタグデータ 312_1 , 312_2 , 312_3 と、署名データ $SIG_{260,SP}$ とを格納したセキュアコンテナ $304a$ を作成する。

ここで、プライスタグデータ 312_1 , 312_2 , 312_3 は、それぞれコンテンツデータ C_1 , C_2 , C_3 の販売価格を示している。

また、署名データ $SIG_{260,SP}$ は、コンテンツファイル CF_{101} , CF_{102} , CF_{103} 、キーファイル KF_{101} , KF_{102} , KF_{103} 、公開鍵証明書データ CER_{SP} と、署名データ $SIG_{61,ESC}$ およびプライスタグデータ 312_1 , 312_2 , 312_3 の全体に対してハッシュ値をとり、サービスプロバイダ 310 の秘密鍵データ $K_{Sp,s}$ を用いて生成される。

【0390】

サービスプロバイダ 310 は、図95に示すセキュアコンテナ $304a$ をユーザホームネットワーク 303 に配給する。

ユーザホームネットワーク 303 では、 $SAM305_1 \sim 305_4$ において、セキュアコンテナ $304a$ に格納された署名データ $SIG_{61,ESC}$ の正当性を確認した後に、公開鍵証明書データ CER_{sp} に格納された公開鍵データ $K_{SP,KP}$ を用いて、署名データ $SIG_{260,SP}$ の正当性を確認する。

その後、 $SAM305_1 \sim 305_4$ は、コンテンツデータ C_{101} , C_{102} , C_{103} についての権利処理を、リンクデータ LD_1 , LD_2 , LD_3 に示されるリンク状態に応じて、それぞれキーファイル KF_{101} , KF_{102} , KF_{103} に基づいて行う。

【0391】

なお、上述した第8変形例では、コンテンツプロバイダ 301 において、図93に示すように、コンテンツプロバイダ 301 において、コンテンツファイル CF_{101} , CF_{102} , CF_{103} 、キーファイル KF_{101} , KF_{102} , KF_{103} 、公開鍵証明書データ CER_{CP} および署名データ $SIG_{1,ESC}$ の全体に対しての署名データ $SIG_{250,CP}$ を作成する場合を例示したが、例えば、コンテンツファイル CF_{101} , CF_{102} , CF_{103} およびキーファイル KF_{101} , KF_{102} , KF_{103} のそれぞれについて署名データを作成し、これをセキュアコンテナ $104a$ 内に格納してもよい。

また、上述した第8変形例では、サービスプロバイダ310において、図95に示すように、コンテンツファイル CF_{101} 、 CF_{102} 、 CF_{103} 、キーファイル KF_{101} 、 KF_{102} 、 KF_{103} 、公開鍵証明書データ CER_{SP} と、署名データ $SIG_{61,ESC}$ およびプライスタグデータ 312_1 、 312_2 、 312_3 の全体に対しての署名データ $SIG_{260,SP}$ を作成する場合を例示したが、これらの各々についての署名データを作成し、これらをセキュアコンテナ304aに格納するようにしてもよい。

【0392】

また、上述した第8変形例では、セキュアコンテナ304において、単数のサービスプロバイダ310から提供を受けた複数のコンテンツファイル CF_{101} 、 CF_{102} 、 CF_{103} を単数のセキュアコンテナ304aに格納してユーザホームネットワーク303に配給する場合を例示したが、図81に示すように、複数のコンテンツプロバイダ301a、301bから提供を受けた複数のコンテンツファイル CF を、単数のセキュアコンテナに格納してユーザホームネットワーク303に配給してもよい。

【0393】

なお、図93に示すフォーマットは、前述した第1実施形態において、図1に示すコンテンツプロバイダ101からユーザホームネットワーク103にセキュアコンテナ104を送信する場合にも同様に適用できる。

【0394】

また、上述した実施形態では、EMDサービスセンタにおいて、SAMから入力した利用履歴データに基づいて決済処理を行う場合を例示したが、SAMにおいてコンテンツの購入形態が決定される度に利用制御状態データをSAMからEMDサービスセンタに送信し、EMDサービスセンタにおいて、受信した利用制御状態データを用いて決済処理を行ってもよい。

【0395】

以下、コンテンツプロバイダ101において作成されるコンテンツファイル C およびキーファイル KF などの概念をまとめる。

コンテンツプロバイダ101がインターネットを用いてコンテンツを提供する

場合には、図96に示すように、ヘッダ、コンテンツID、コンテンツ鍵データKcを用いた暗号化されたコンテンツデータCおよび署名データを含むコンテンツファイルCFが作成される。当該コンテンツデータCの取り扱いを示す権利書データと、コンテンツ鍵データKcとが、所定の信頼機関であるEMDサービスセンタ102、302の配信用鍵データによって暗号化された後に、キーファイルKFに格納される。また、キーファイルKFには、ヘッダ、コンテンツID、必要に応じてメタデータ、署名データが格納される。

そして、コンテンツファイルCFおよびキーファイルKFが、コンテンツプロバイダ101からユーザホームネットワーク103、303に直接提供されたり、コンテンツプロバイダ101からサービスプロバイダ310を介してユーザホームネットワーク103、303に提供される。

【0396】

また、コンテンツプロバイダ101がインターネットを用いてコンテンツを提供する場合に、図97に示すように、キーファイルKF内にコンテンツ鍵データKcを格納しないで、所定の信頼機関であるEMDサービスセンタ102、302の配信用鍵データによって暗号化したコンテンツ鍵データKcをEMDサービスセンタ102、302からユーザホームネットワーク103、303に提供してもよい。

【0397】

また、コンテンツプロバイダ101がデジタル放送を用いてコンテンツを提供する場合に、例えば、図98に示すように、コンテンツ鍵データKcを用いて暗号化したコンテンツデータCと署名データとを、コンテンツプロバイダ101からユーザホームネットワーク103、303に、直接あるいはサービスプロバイダ310を介して提供する。この場合に、図97に示すキーファイルKFに対応する鍵データブロックを、コンテンツプロバイダ101からユーザホームネットワーク103、303に、直接あるいはサービスプロバイダ310を介して提供する。

また、この場合に、例えば、図99に示すように、所定の信頼機関であるEMDサービスセンタ102、302の配信用鍵データによって暗号化したコンテ

ツ鍵データKcをEMDサービスセンタ102, 302からユーザホームネットワーク103, 303に提供してもよい。

【0398】

【発明の効果】

以上説明したように、本発明によれば、データ提供装置の関係者の利益が適切に保護される。

また、本発明によれば、権利書データなどが不正に改竄されることを適切に回避できる。

また、本発明によれば、データ提供装置の関係者の利益を保護するための監査の負担を軽減できる。

【図面の簡単な説明】

【図1】

図1は、本発明の第1実施形態のEMDシステムの全体構成図である。

【図2】

図2は、図1に示すコンテンツプロバイダの機能ブロック図であり、ユーザホームネットワークのSAMとの間で送受信されるデータに関連するデータの流れを示す図である。

【図3】

図3は、図1に示すコンテンツプロバイダの機能ブロック図であり、コンテンツプロバイダとEMDサービスセンタとの間で送受信されるデータに関連するデータの流れを示す図である。

【図4】

図4は、図1に示すコンテンツプロバイダからSAMに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図5】

図5は、OSIレイヤ層と、本実施形態のセキュアコンテナの定義との対応関係を説明するための図である。

【図6】

図6は、ROM型の記録媒体を説明するための図である。

【図 7】

図 7 (A) はコンテンツプロバイダから EMD サービスセンタに送信される権利登録要求用モジュールのフォーマットを説明するための図、図 7 (B) は EMD サービスセンタからコンテンツプロバイダに送信される権利化証明書モジュールを説明するための図である。

【図 8】

図 8 は、第 1 実施形態において、コンテンツプロバイダが、EMD サービスセンタに、自らの秘密鍵データに対応する公開鍵データの正当性を証明する公開鍵証明書データを要求する場合の処理のフローチャートである。

【図 9】

図 9 は、第 1 実施形態において、コンテンツプロバイダがユーザホームネットワークの SAM にセキュアコンテナを送信する場合の処理のフローチャートである。

【図 10】

図 10 は、図 1 に示す EMD サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 11】

図 11 は、図 1 に示す EMD サービスセンタの機能ブロック図であり、SAM および図 1 に示す決済機関との間で送受信されるデータに関連するデータの流れを示す図である。

【図 12】

図 12 は、第 1 実施形態において、EMD サービスセンタがコンテンツプロバイダから公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

【図 13】

図 13 は、第 1 実施形態において、EMD サービスセンタが SAM から、公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

【図 1 4】

図 1 4 は、第 1 実施形態において、EMD サービスセンタがコンテンツプロバイダから権利書データおよびコンテンツ鍵データの登録要求を受けた場合の処理のフローチャートである。

【図 1 5】

図 1 5 は、第 1 実施形態において、EMD サービスセンタが決済処理を行なう場合の処理のフローチャートである。

【図 1 6】

図 1 6 は、図 1 に示すユーザホームネットワーク内のネットワーク機器の構成図である。

【図 1 7】

図 1 7 は、図 1 に示すユーザホームネットワーク内の SAM の機能ブロック図であり、コンテンツプロバイダから受信したセキュアコンテナを復号するまでのデータの流れを示す図である。

【図 1 8】

図 1 8 は、図 1 6 に示す外部メモリに記憶されるデータを説明するための図である。

【図 1 9】

図 1 9 は、スタックメモリに記憶されるデータを説明するための図である。

【図 2 0】

図 2 0 は、図 1 に示すユーザホームネットワーク内のネットワーク機器のその他の構成図である。

【図 2 1】

図 2 1 は、図 1 7 に示す記憶部に記憶されるデータを説明するための図である。

【図 2 2】

図 2 2 は、第 1 実施形態において、セキュアコンテナをコンテンツプロバイダから入力し、セキュアコンテナ内のキーファイル KF を復号する際の SAM 内での処理のフローチャートである。

【図 2 3】

図 2 3 は、図 1 に示すユーザホームネットワーク内の S A M の機能ブロック図であり、コンテンツデータを利用・購入する処理などに関連するデータの流れを示す図である。

【図 2 4】

図 2 4 は、第 1 実施形態において、コンテンツプロバイダからダウンロードメモリにダウンロードされたセキュアコンテナの購入形態を決定するまでの処理のフローチャートである。

【図 2 5】

図 2 5 は、第 1 実施形態において、ダウンロードメモリに記憶されている購入形態が既に決定されたコンテンツデータを再生する場合の処理のフローチャートである。

【図 2 6】

図 2 6 は、図 1 6 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、A V 機器の S A M に転送する場合の転送元の S A M 内での処理の流れを説明するための図である。

【図 2 7】

図 2 7 は、図 2 6 に示す場合における転送元の S A M 内でのデータの流れを示す図である。

【図 2 8】

図 2 8 は、第 1 実施形態において、ネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルおよびキーファイルを、他の A V 機器の S A M に転送する場合の S A M 内での処理のフローチャートである。

【図 2 9】

図 2 9 は、購入形態が決定したセキュアコンテナのフォーマットを説明するための図である。

【図 3 0】

図 3 0 は、図 2 6 に示す場合において、転送先の S A M において、入力したコ

コンテンツファイルなどを、RAM型あるいはROM型の記録媒体（メディア）に書き込む際のデータの流れを示す図である。

【図 3 1】

図 3 1 は、第 1 実施形態において、他の SAM から入力したコンテンツファイルなどを、RAM 型などの記録媒体に書き込む際の SAM 内での処理のフローチャートである。

【図 3 2】

図 3 2、コンテンツの購入形態が未決定の図 6 に示す ROM 型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV 機器において購入形態を決定する際の処理の流れを説明するための図である。

【図 3 3】

図 3 3 は、図 3 2 に示す場合において、SAM 内でのデータの流れを示す図である。

【図 3 4】

図 3 4 は、第 1 実施形態において、コンテンツの購入形態が未決定の図 5 に示す ROM 型の記録媒体をユーザホームネットワークがオフラインで配給を受けた場合に、AV 機器において購入形態を決定する際の処理のフローチャートである。

【図 3 5】

図 3 5 は、図 3 4 のフローチャートの続きのフローチャートである。

【図 3 6】

図 3 6 は、ユーザホームネットワーク内の AV 機器において購入形態が未決定の ROM 型の記録媒体からセキュアコンテナを読み出して、これを他の AV 機器に転送して RAM 型の記録媒体に書き込む際の処理の流れを説明するための図である。

【図 3 7】

図 3 7 は、図 3 6 に示すように、第 1 の AV 機器において購入形態が未決定の ROM 型の記録媒体からセキュアコンテナを読み出して第 2 の AV 機器に転送し、第 2 の AV 機器において購入形態を決定して RAM 型の記録媒体に書き込む際

の第1のAV機器の処理のフローチャートである。

【図38】

図38は、図37に示す場合の第2のAV機器の処理のフローチャートである。

【図39】

図39は、図38に示すフローチャートの続きのフローチャートである。

【図40】

図40は、図36に示す場合における転送元のSAM内でのデータの流れを示す図である。

【図41】

図41は、図36に示す場合における転送先のSAM内でのデータの流れを示す図である。

【図42】

図42は、図1に示すコンテンツプロバイダ、EMDサービスセンタおよびSAMの相互間で、イン・バンド方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図43】

図43は、図1に示すコンテンツプロバイダ、EMDサービスセンタおよびSAMの相互間で、イン・バンド方式およびアウト・バンド方式で、送受信されるデータのフォーマットを説明するための図である。

【図44】

図44は、バスへの機器の接続形態の一例を説明するための図である。

【図45】

図45は、SAM登録リストのデータフォーマットを説明するための図である。

【図46】

図46は、図1に示すコンテンツプロバイダの全体動作のフローチャートである。

【図 4 7】

図 4 7 は、本発明の第 1 実施形態の第 2 変形例を説明するための図である。

【図 4 8】

図 4 8 は、本発明の第 1 実施形態の第 3 変形例を説明するための図である。

【図 4 9】

図 4 9 は、本発明の第 2 実施形態の EMD システムの全体構成図である。

【図 5 0】

図 5 0 は、図 4 9 に示すコンテンツプロバイダの機能ブロック図であり、サービスプロバイダに送信されるセキュアコンテナに関するデータの流れを示す図である。

【図 5 1】

図 5 1 は、図 4 9 に示すサービスプロバイダの機能ブロック図であり、ユーザホームネットワークとの間で送受信されるデータの流れを示す図である。

【図 5 2】

図 5 2 は、第 2 実施形態において、コンテンツプロバイダから供給を受けたセキュアコンテナからセキュアコンテナを作成し、これをユーザホームネットワークに配給する際のサービスプロバイダの処理のフローチャートである。

【図 5 3】

図 5 3 は、図 4 9 に示すサービスプロバイダからユーザホームネットワークに送信されるセキュアコンテナのフォーマットを説明するための図である。

【図 5 4】

図 5 4 は、図 4 9 に示すサービスプロバイダの機能ブロック図であり、EMD サービスセンタとの間で送受信されるデータの流れを示す図である。

【図 5 5】

図 5 5 は、サービスプロバイダから EMD サービスセンタに送信されるプライスタグ登録要求用モジュールのフォーマットを説明するための図である。

【図 5 6】

図 5 6 は、図 4 9 に示す EMD サービスセンタの機能ブロック図であり、サービスプロバイダとの間で送受信されるデータに関連するデータの流れを示す図で

ある。

【図 5 7】

図 5 7 は、図 4 9 に示す EMD サービスセンタの機能ブロック図であり、コンテンツプロバイダとの間で送受信されるデータに関連するデータの流れを示す図である。

【図 5 8】

図 5 8 は、図 4 9 に示す EMD サービスセンタの機能ブロック図であり、SAM との間に送受信されるデータに関連するデータの流れを示す図である。

【図 5 9】

図 5 9 は、利用履歴データの内容を説明するための図である。

【図 6 0】

図 6 0 は、第 2 実施形態において、EMD サービスセンタがサービスプロバイダから公開鍵証明書データの発行要求を受けた場合の処理のフローチャートである。

【図 6 1】

図 6 1 は、第 2 実施形態において、EMD サービスセンタが、サービスプロバイダからプライスタグデータの登録要求を受けた場合の処理のフローチャートである。

【図 6 2】

図 6 2 は、第 2 実施形態において、EMD サービスセンタが決済を行なう場合の処理のフローチャートである。

【図 6 3】

図 6 3 は、図 4 9 に示すネットワーク機器の構成図である。

【図 6 4】

図 6 4 は、図 6 3 に示す CA モジュールの機能ブロック図である。

【図 6 5】

図 6 5 は、図 6 3 に示す SAM の機能ブロック図であり、セキュアコンテナを入力してから復号するまでのデータの流れを示す図である。

【図 6 6】

図 6 6 は、図 6 5 に示す記憶部に記憶されるデータを説明するための図である。

【図 6 7】

図 6 7 は、図 6 3 に示す SAM の機能ブロック図であり、コンテンツの購入・利用形態を決定する場合などのデータの流れを示す図である。

【図 6 8】

図 6 8 は、第 2 実施形態において、セキュアコンテナをサービスプロバイダから入力し、セキュアコンテナ内のキーファイルを復号する際の SAM の処理のフローチャートである。

【図 6 9】

図 6 9 は、第 2 実施形態において、サービスプロバイダからダウンロードメモリにダウンロードされたセキュアコンテナの購入形態を決定するまでの SAM の処理のフローチャートである。

【図 7 0】

図 7 0 は、ダウンロードメモリに記憶されている購入形態が既に決定されたコンテンツデータを再生する場合の処理のフローチャートである。

【図 7 1】

図 7 1 は、購入形態が決定された後のキーファイルのフォーマットを説明するための図である。

【図 7 2】

図 7 2 は、図 6 3 に示すネットワーク機器のダウンロードメモリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、AV 機器の SAM に転送する場合の転送先の SAM 内での処理の流れを説明するための図である。

【図 7 3】

図 7 3 は、図 7 2 に示す場合の転送元の SAM 内でのデータの流れを示す図である。

【図 7 4】

図 7 4 は、図 7 2 に示すように、例えば、ネットワーク機器のダウンロードメ

モリにダウンロードされた既に購入形態が決定されたコンテンツファイルを、A V機器のSAMに転送する場合の転送元のSAMの処理のフローチャートである。

【図 7 5】

図 7 5 は、ネットワーク機器のSAMからA V機器のSAMに転送される購入形態が既に決定されたセキュアコンテナのフォーマットを説明するための図である。

【図 7 6】

図 5 1 は、図 7 2 に示す場合の転送先のSAM内でのデータの流れを示す図である。

【図 7 7】

図 7 7 は、図 7 2 に示すように、他のSAMから入力したコンテンツファイルなどを、RAM型などの記録媒体に書き込む際のSAMの処理のフローチャートである。

【図 7 8】

図 7 8 は、図 4 9 に示すEMDシステムの全体動作のフローチャートである。

【図 7 9】

図 7 9 は、図 4 9 に示すEMDシステムの全体動作のフローチャートである。

【図 8 0】

図 8 0 は、本発明の第 2 実施形態の第 1 変形例に係わる 2 個のサービスプロバイダを用いたEMDシステムの構成図である。

【図 8 1】

図 8 1 は、本発明の第 2 実施形態の第 2 変形例に係わる複数のコンテンツプロバイダを用いたEMDシステムの構成図である。

【図 8 2】

図 8 2 は、本発明の第 2 実施形態の第 3 変形例に係わるEMDシステムの構成図である。

【図 8 3】

図 8 3 は、本発明の第 2 実施形態の第 4 変形例に係わるEMDシステムの構成

図である。

【図 8 4】

図 8 4 は、公開鍵証明書データの取得ルートの形態を説明するための図である。

【図 8 5】

図 8 5 は、コンテンツプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 8 6】

図 8 6 は、サービスプロバイダの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 8 7】

図 8 7 は、SAMの公開鍵証明書データを無効にする場合の処理を説明するための図である。

【図 8 8】

図 8 8 は、SAMの公開鍵証明書データを無効にする場合のその他の処理を説明するための図である。

【図 8 9】

図 8 9 は、図 4 9 に示す EMD システムにおいて、EMD サービスセンタの代わりに権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを設けた場合を説明するための図である。

【図 9 0】

図 9 0 は、図 8 9 に示す権利管理用クリアリングハウスおよび電子決済用クリアリングハウスを単体の EMD サービスセンタ内に設けた場合の EMD システムの構成図である。

【図 9 1】

図 9 1 は、サービスプロバイダが電子決済用クリアリングハウスに直接的に決済を行う場合の EMD システムの構成図である。

【図 9 2】

図 9 2 は、コンテンツプロバイダが電子決済用クリアリングハウスに直接的に

決済を行う場合のEMDシステムの構成図である。

【図 9 3】

図 9 3 は、本発明の第 2 実施形態の第 8 変形例において、図 4 9 に示すコンテンツプロバイダからサービスプロバイダに提供されるセキュアコンテナのフォーマットを説明するための図である。

【図 9 4】

図 9 4 は、図 9 3 に格納されたモジュールの詳細なフォーマットを説明するための図である。

【図 9 5】

図 9 5 は、本発明の第 2 実施形態の第 8 変形例において、図 4 9 に示すサービスプロバイダから SAM に提供されるセキュアコンテナのフォーマットを説明するための図である。

【図 9 6】

図 9 6 は、インターネットを用いてセキュアコンテナを提供する場合の概念図である。

【図 9 7】

図 9 7 は、インターネットを用いてセキュアコンテナを提供する場合のその他の概念図である。

【図 9 8】

図 9 8 は、デジタル放送を用いてセキュアコンテナを提供する場合の概念図である。

【図 9 9】

図 9 9 は、デジタル放送を用いてセキュアコンテナを提供する場合のその他の概念図である。

【図 1 0 0】

図 1 0 0 は、従来の EMD システムの構成図である。

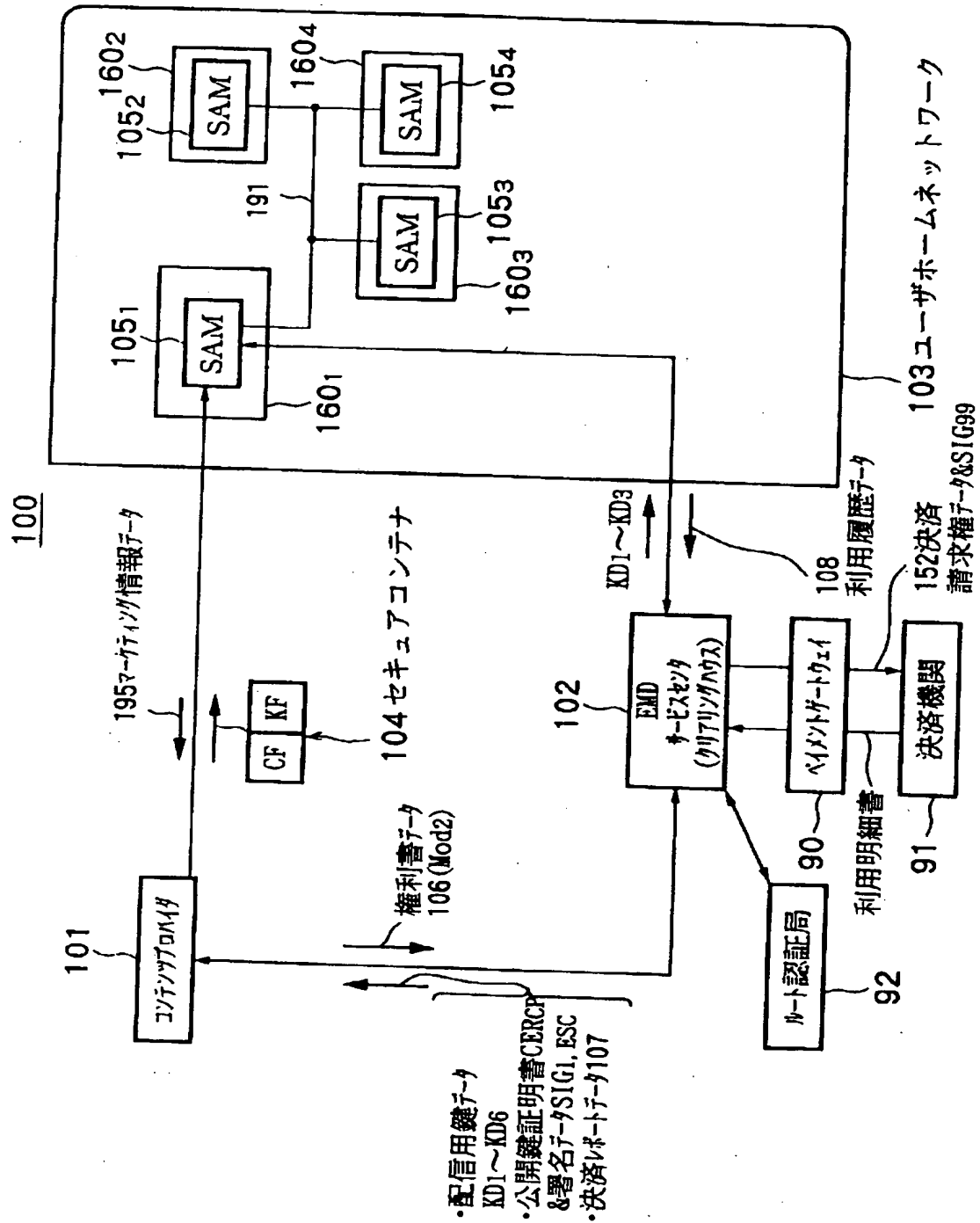
【符号の説明】

9 0 … ペイメントゲートウェイ、9 1 … 決済機関、9 2 … ルート認証局、1 0 0, 3 0 0 … EMD システム、1 0 1, 3 0 1 … コンテンツプロバイダ、1 0 2

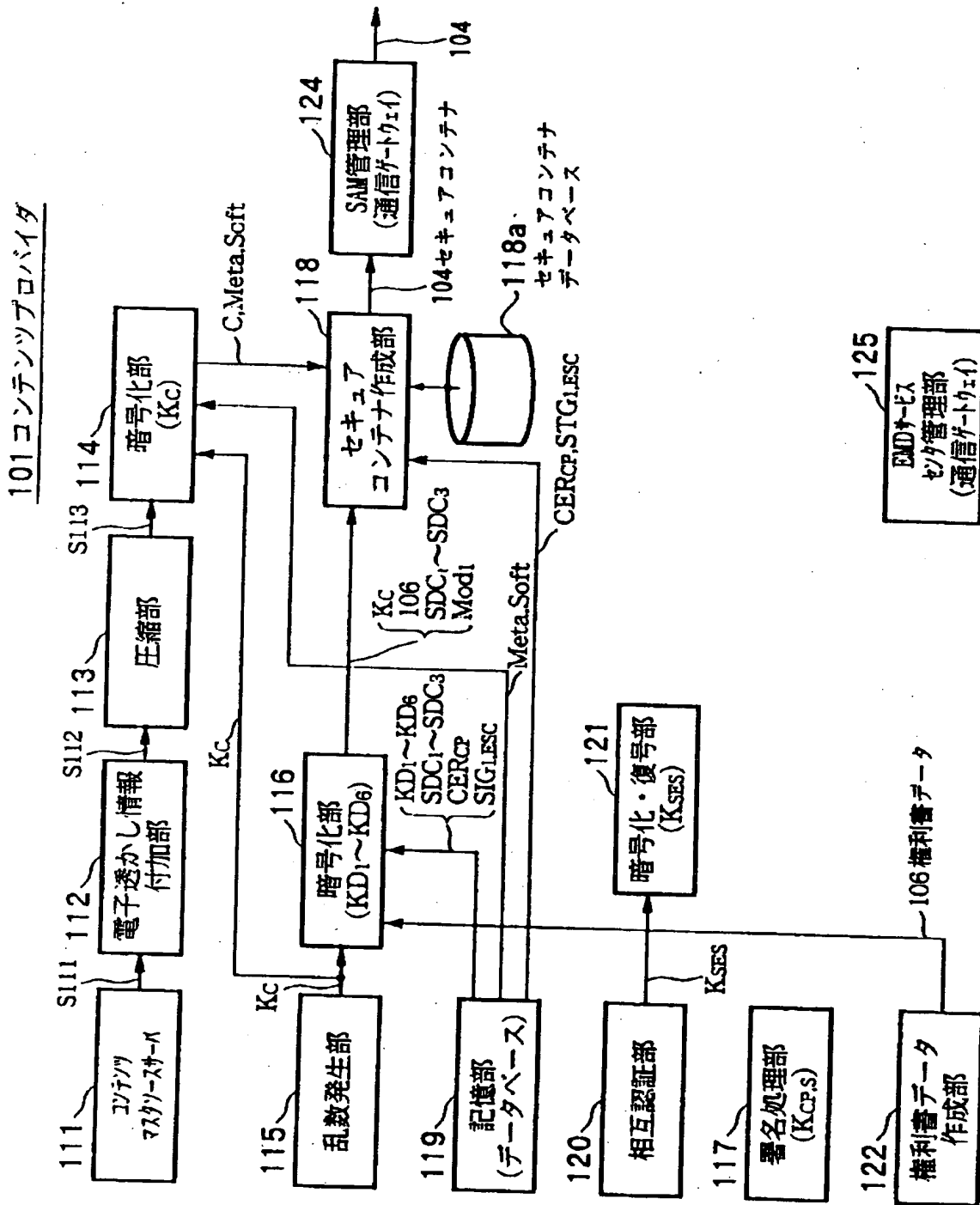
、302…EMDサービスセンタ、103、303…ユーザホームネットワーク、104、304…セキュアコンテナ、105₁～105₄、305₁～305₄…SAM、106…権利書データ、107、307…決済レポートデータ、108、308…利用履歴データ、160₁…ネットワーク機器、160₂～160₄…AV機器、152、152c、152s…決済請求権データ、191…バス、310…サービスプロバイダ、311…CAモジュール、312…プライスタグデータ、CF…コンテンツファイル、KF…キーファイル、Kc…コンテンツ鍵データ

【書類名】 図面

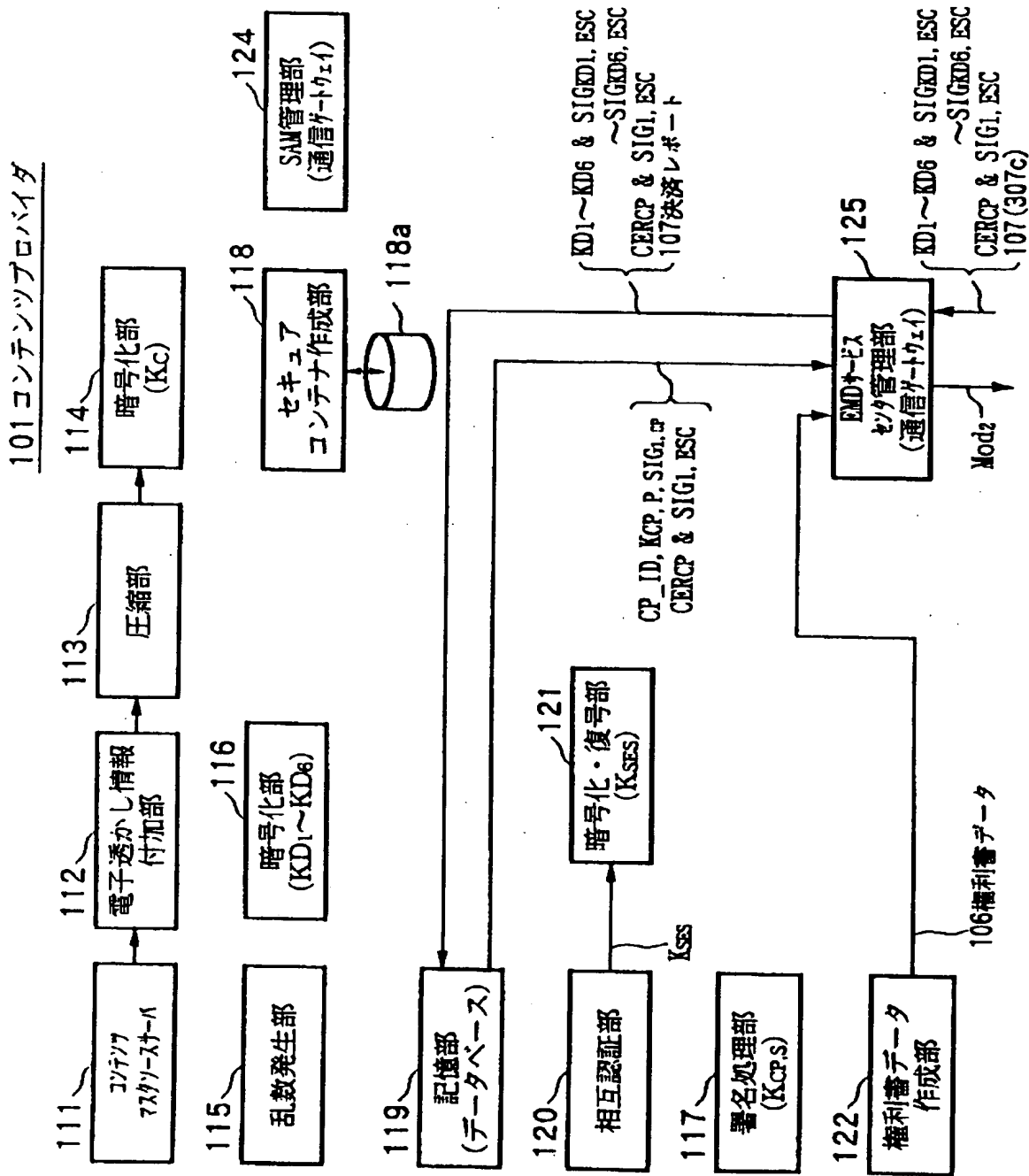
【図1】



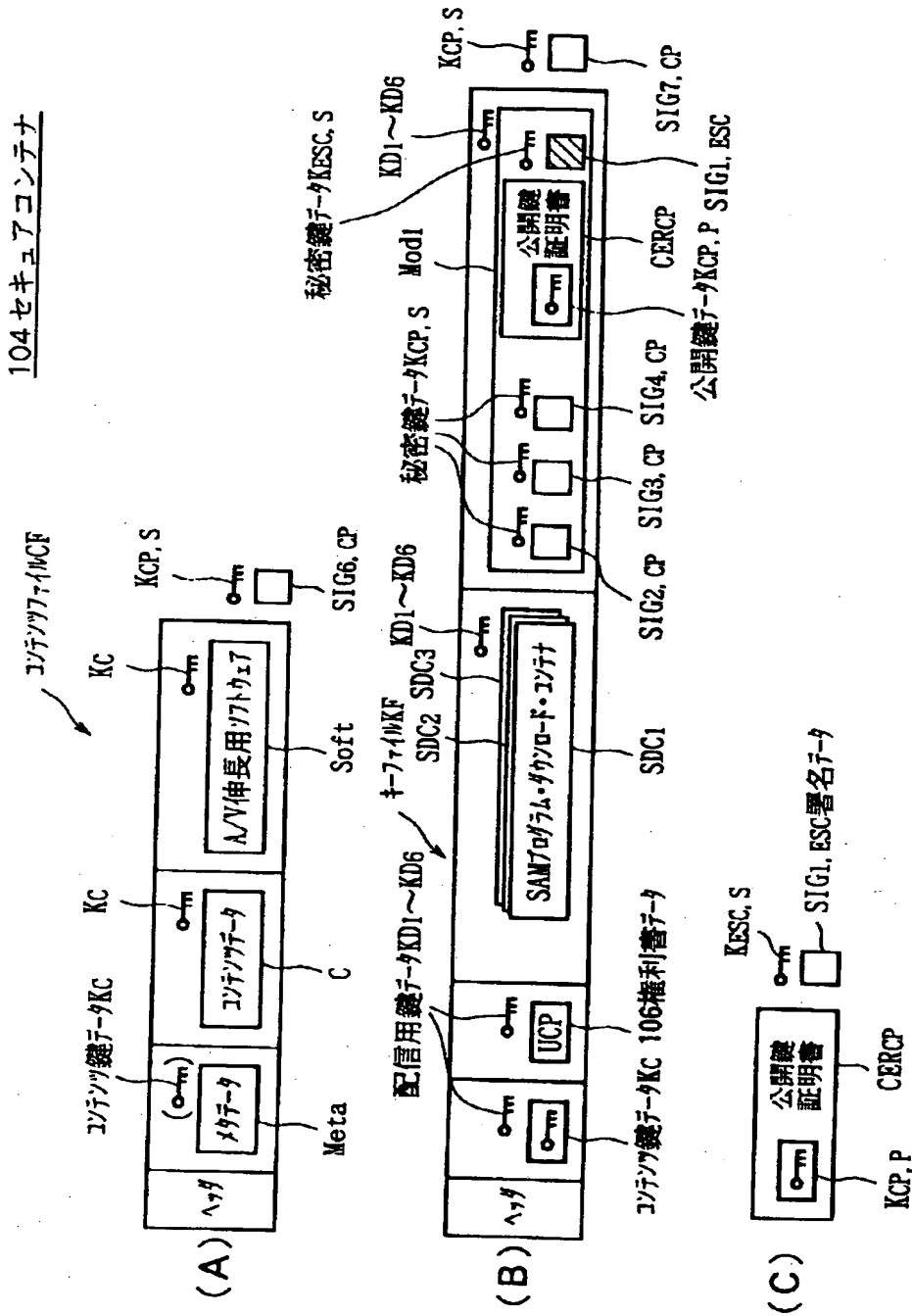
【図 2】



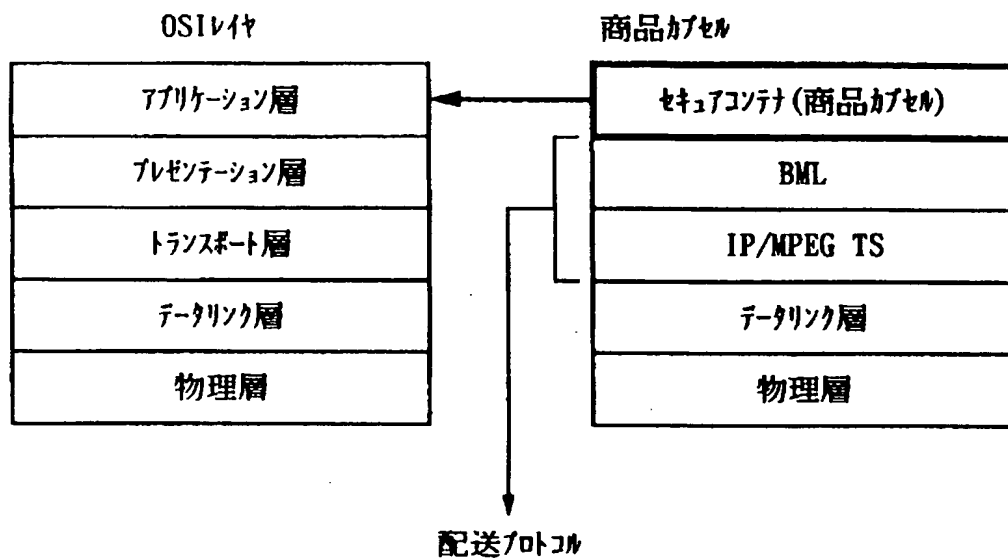
【図3】



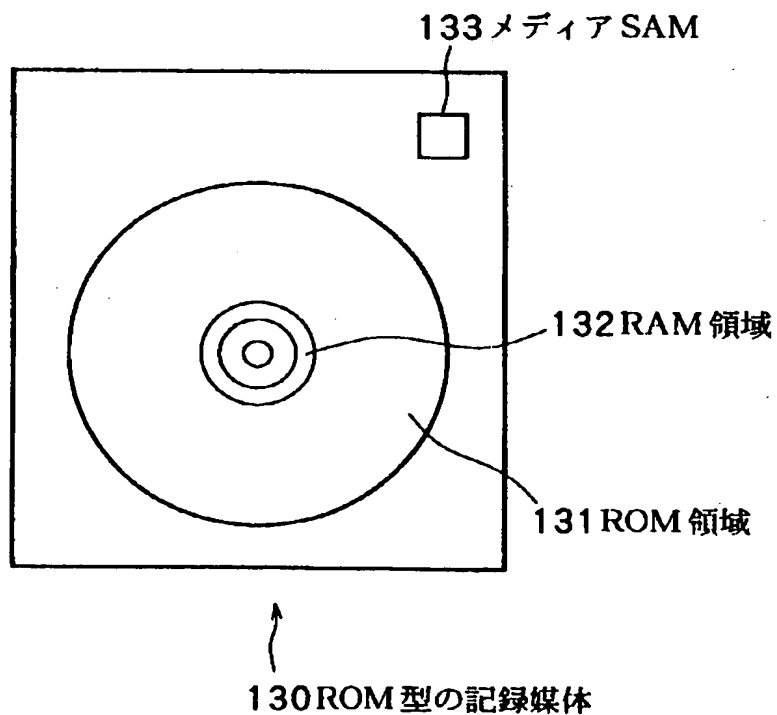
【図 4】



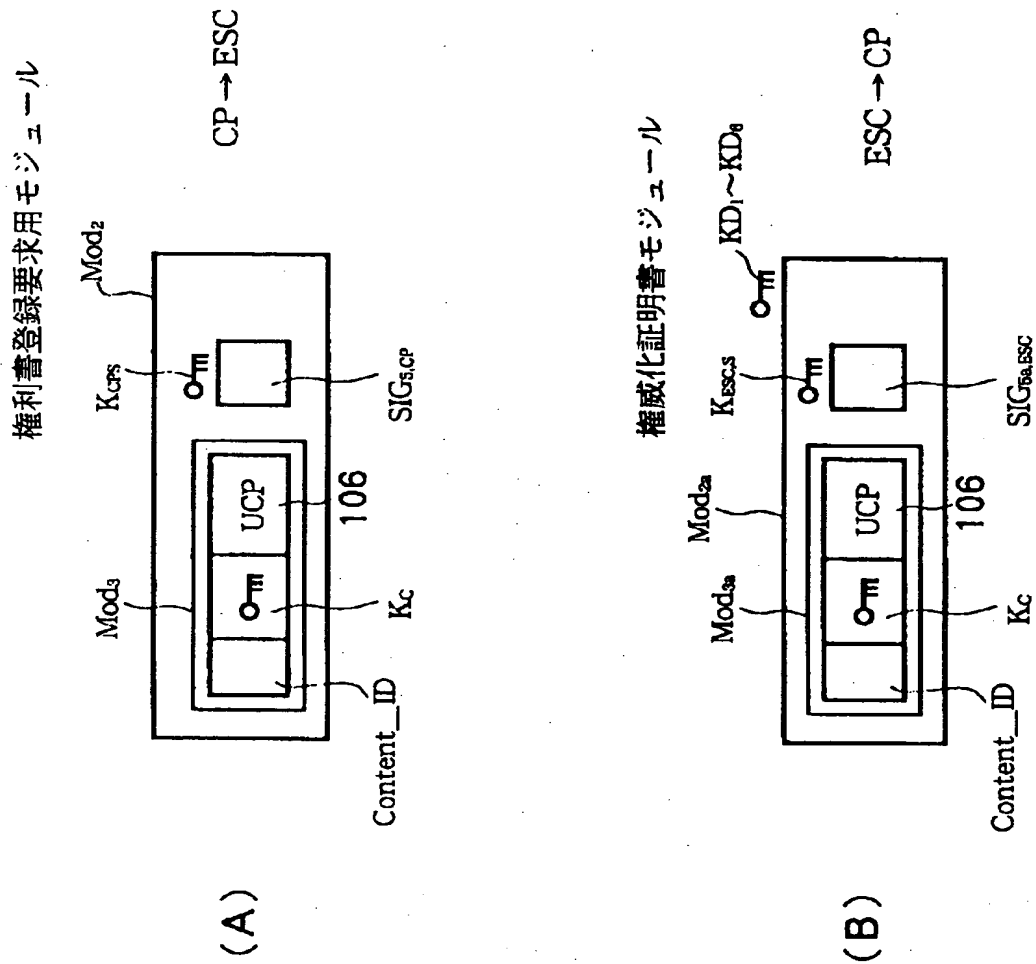
【図 5】



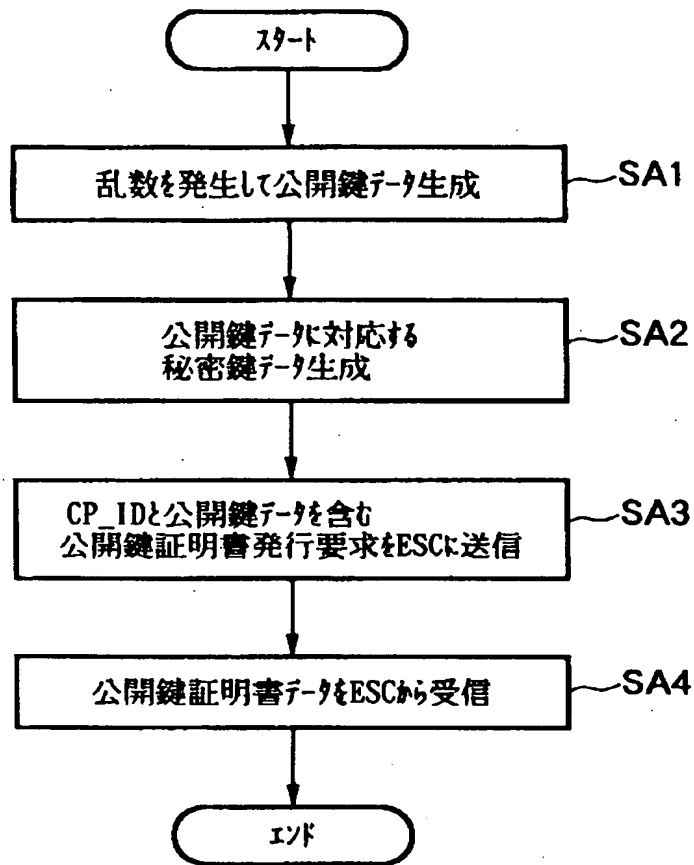
【図 6】



【図 7】

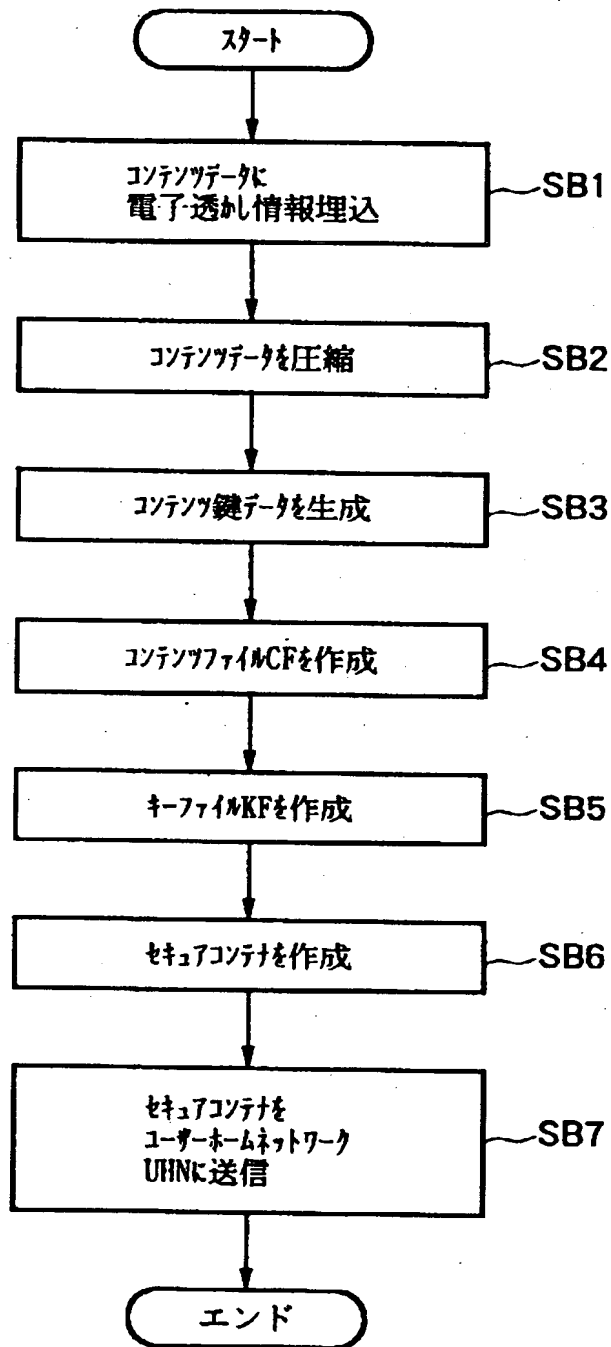


【図 8】



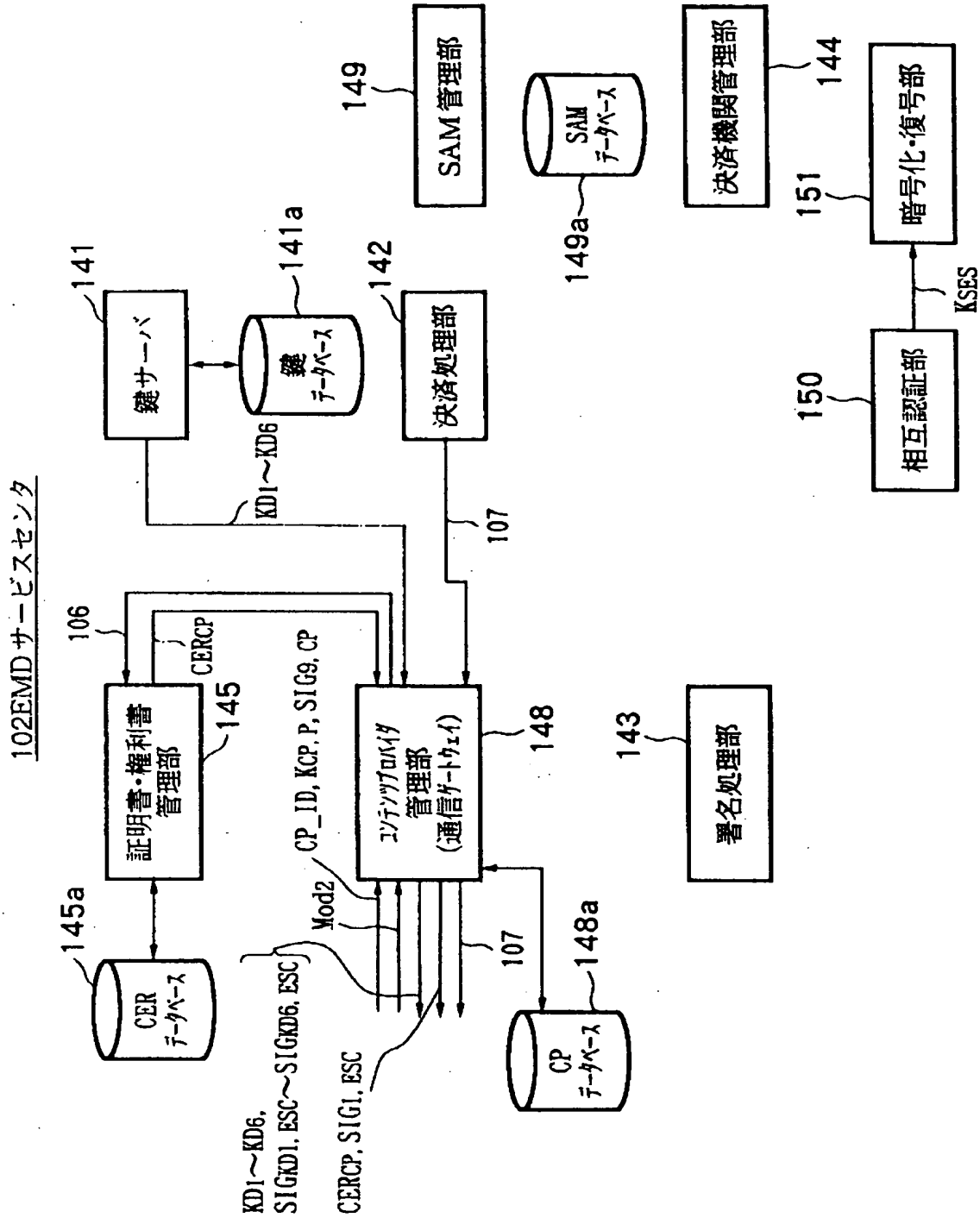
CPからESCへの公開鍵証明書データの発行要求処理

【図9】



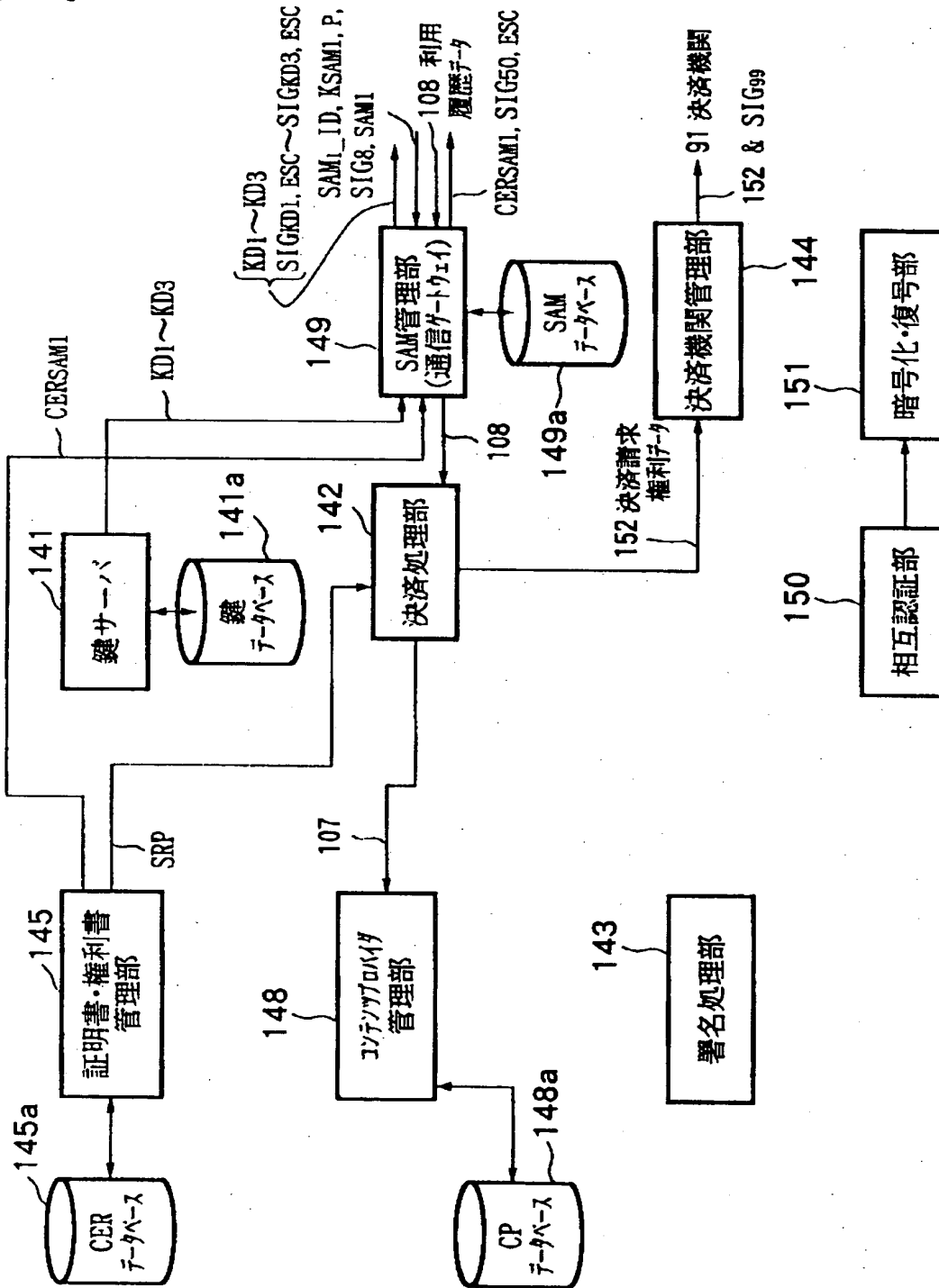
CPのセキュアコンテナ作成処理

【図10】

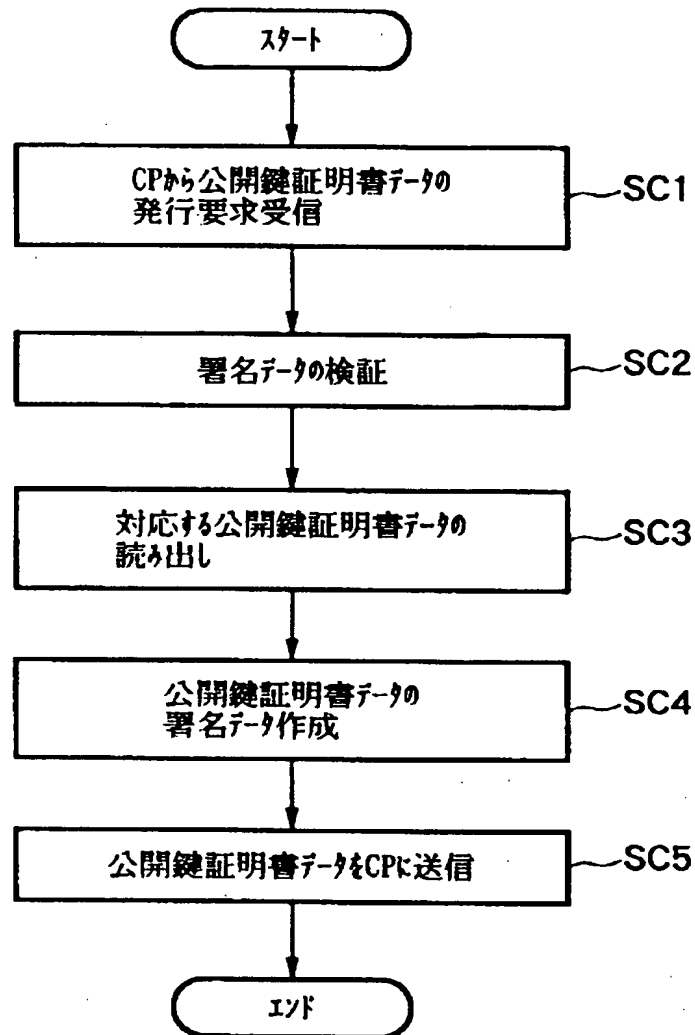


【図11】

102EMD サービスセンタ

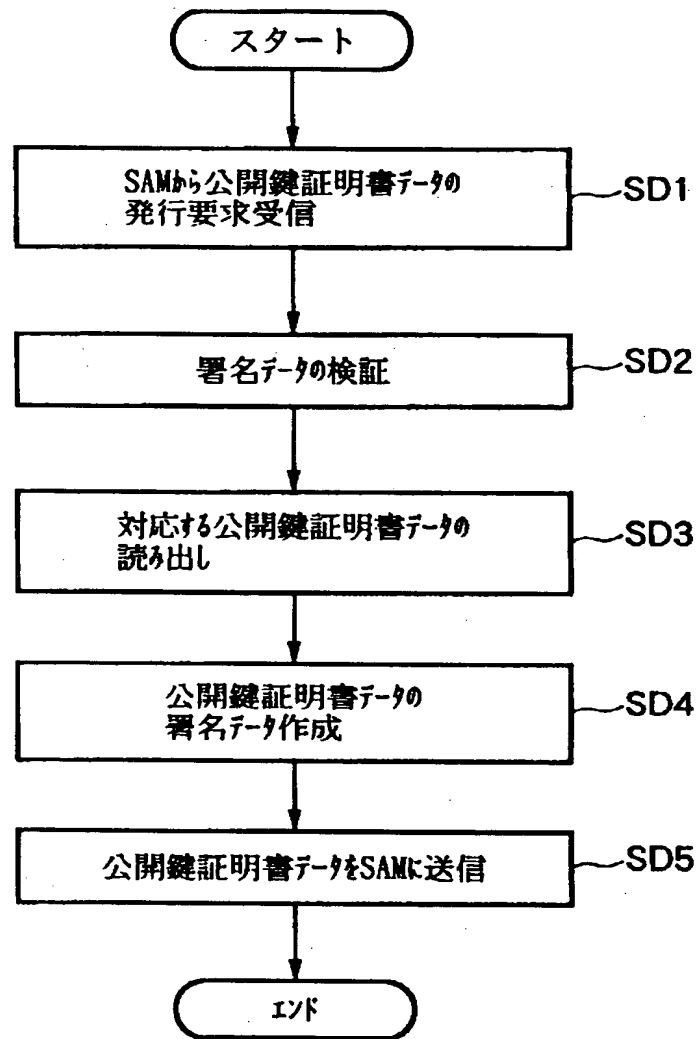


【図 12】



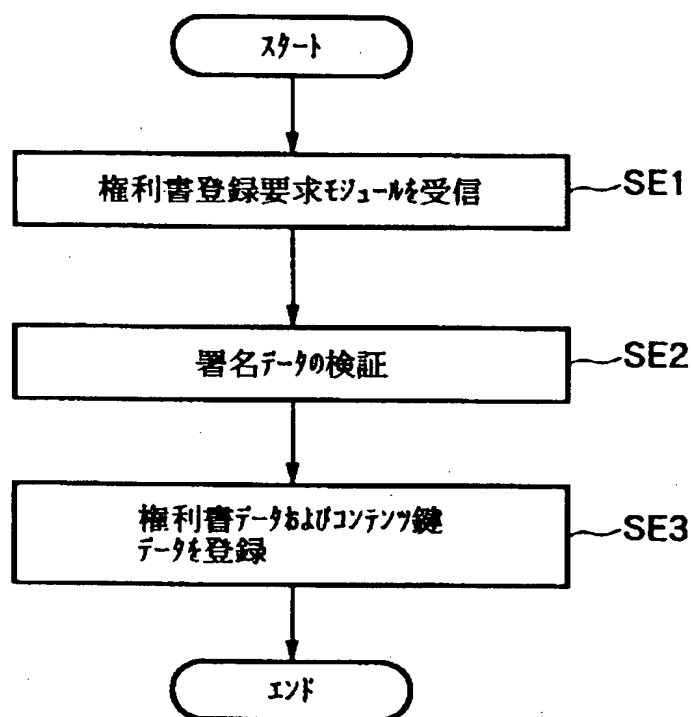
CPからの公開鍵証明書データの発行要求に応じたESCの処理

【図 13】



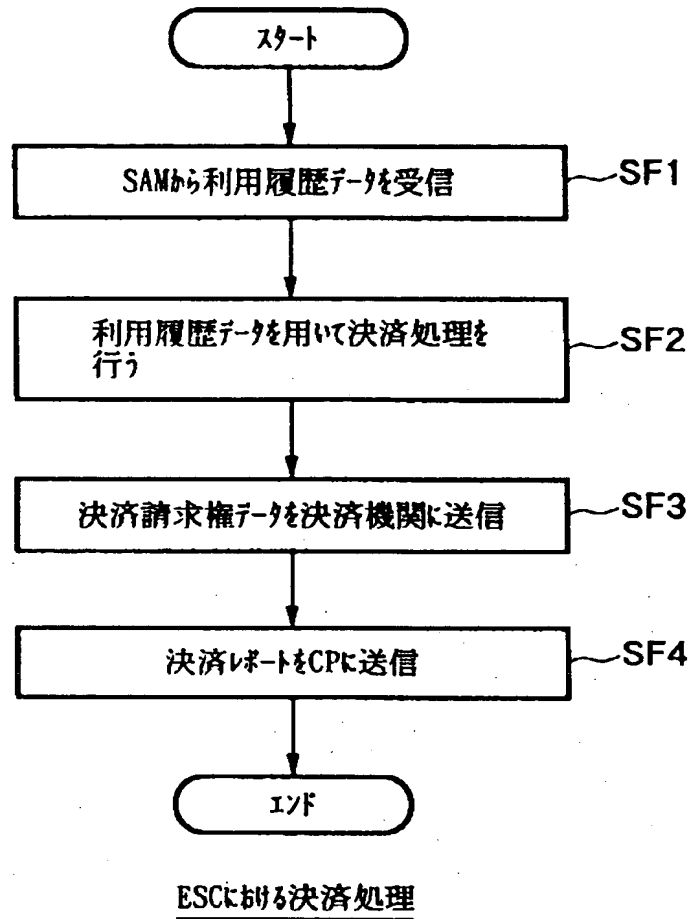
SAMからの公開鍵証明書データの発行要求に応じたESCの処理

【図14】

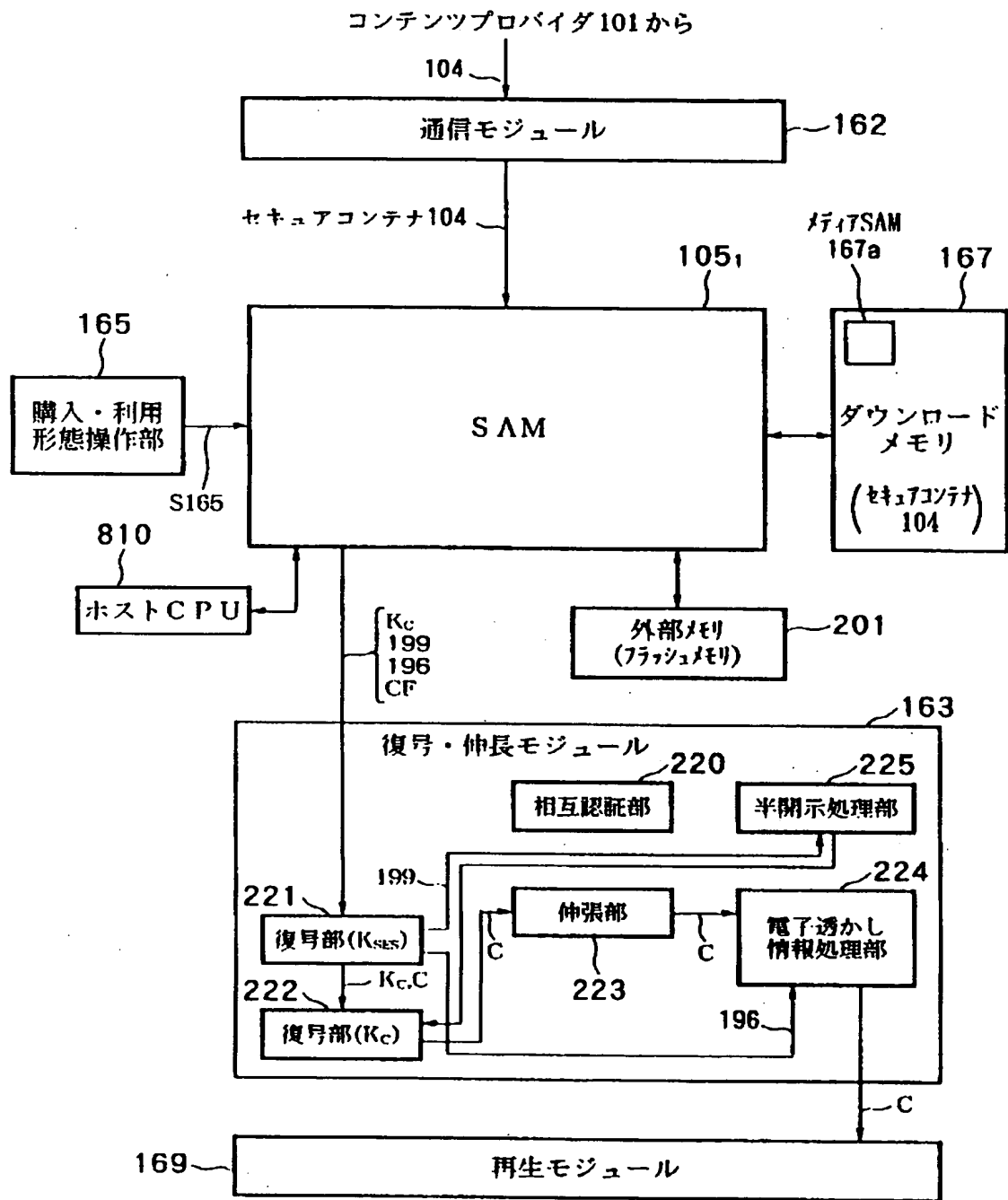


ESCにおける権利書データおよびコンテンツ鍵データの登録処理

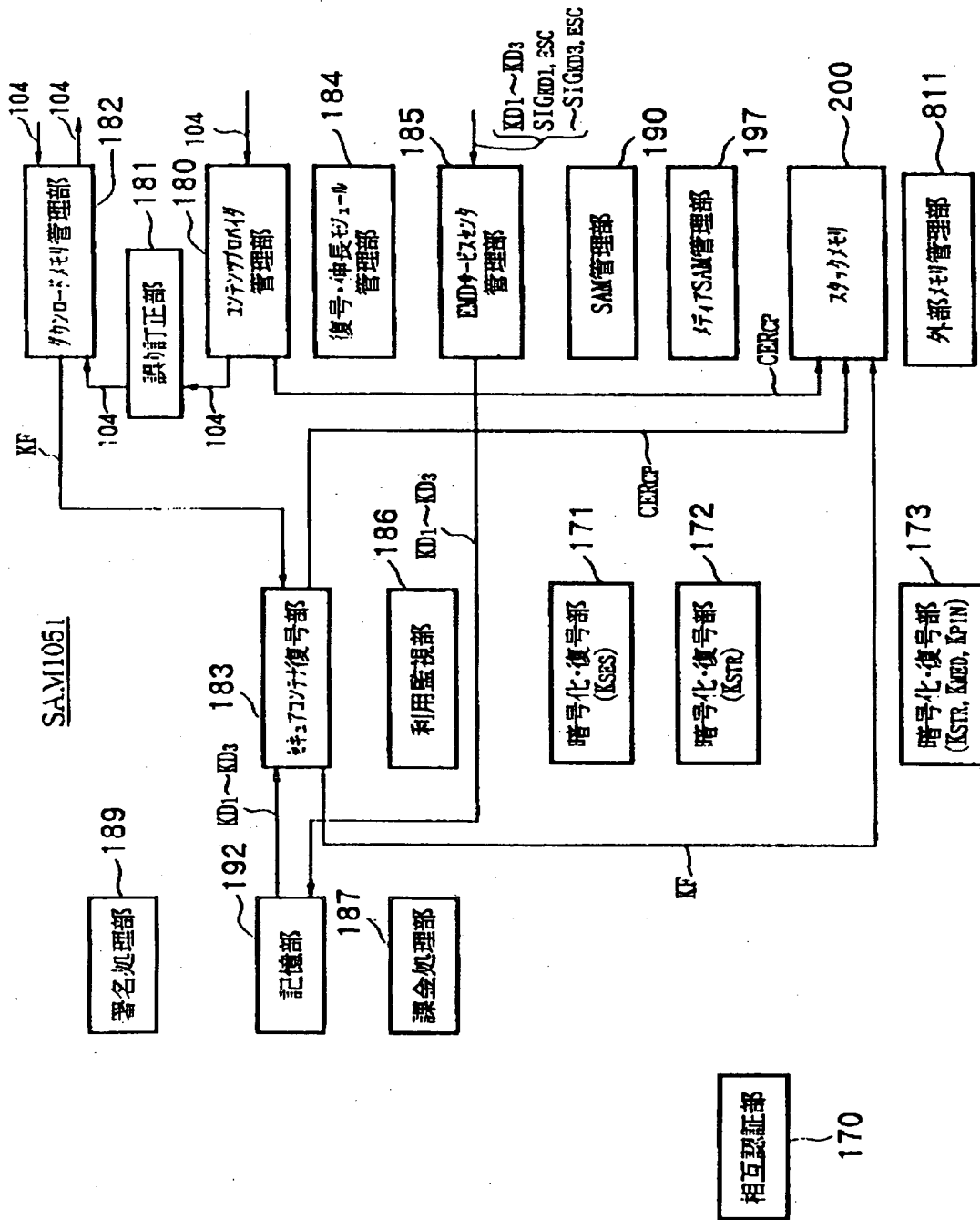
【図15】



【図16】



【図 17】



【図 18】

外部メモリ 201 に記憶されるデータ

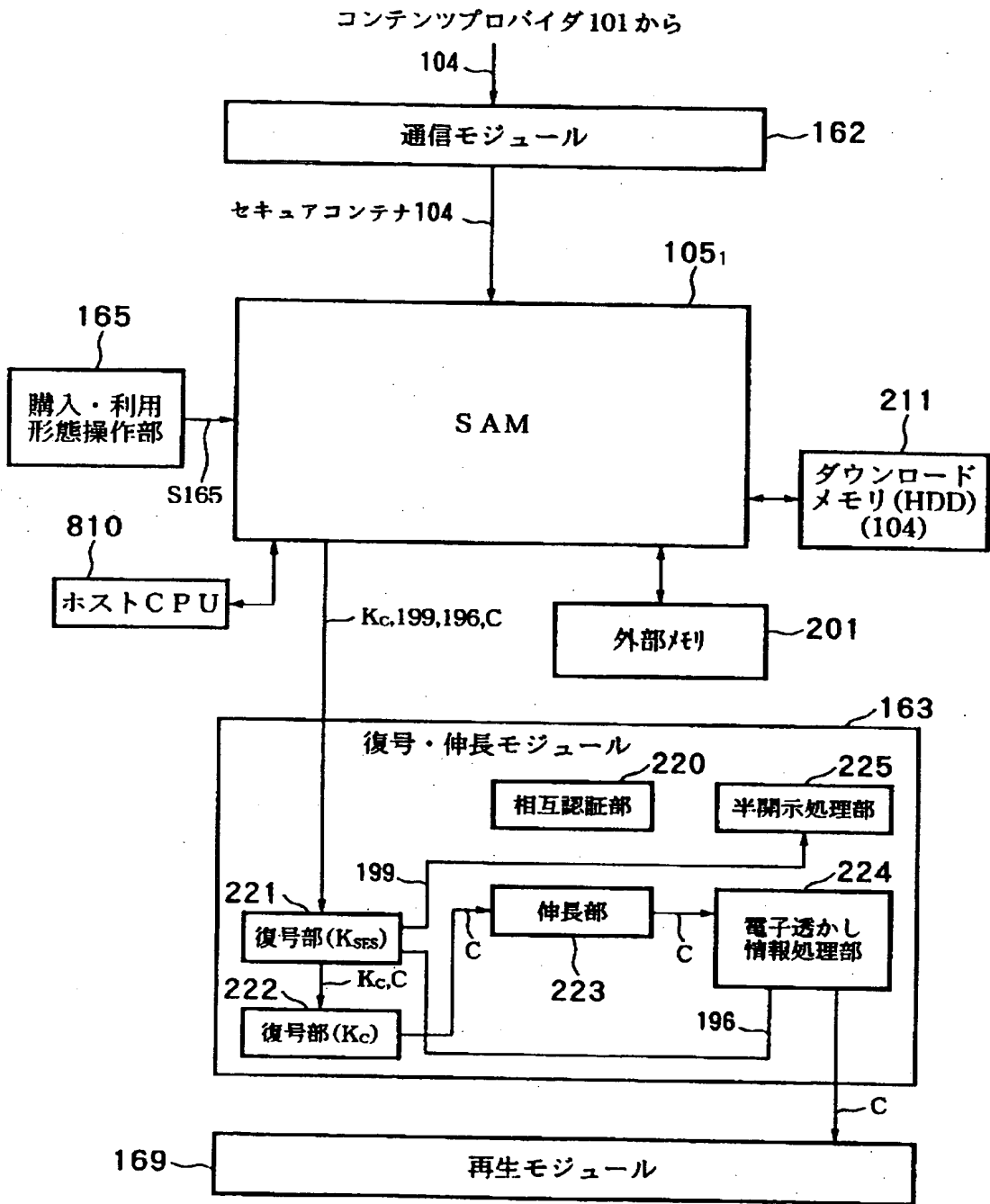
利用履歴データ 108
SAM 登録リスト

【図 19】

スタックメモリ 200 に記憶されるデータ

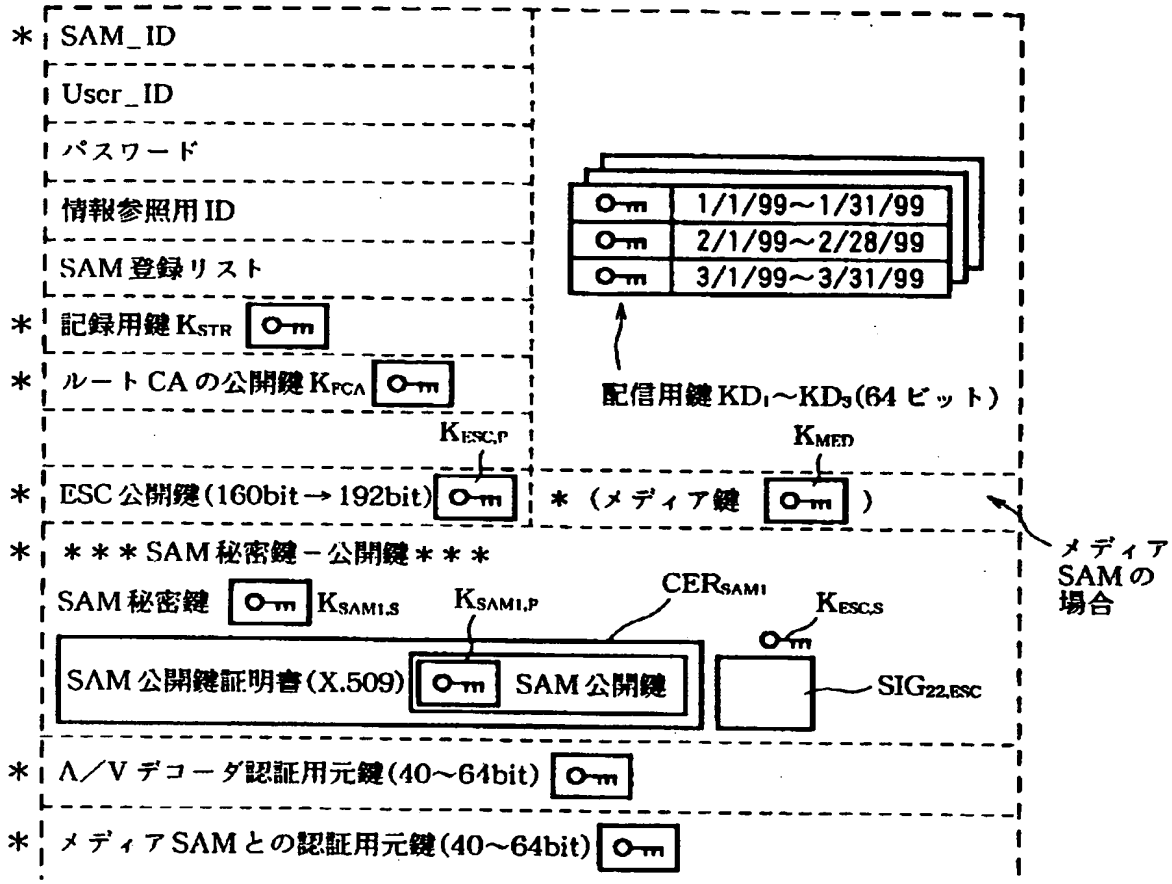
コンテンツ鍵データ K_c
権利書データ (UCP) 106
記憶部 (フラッシュメモリ) 192 のロック鍵データ K_{LOC}
コンテンツプロバイダ 101 の公開鍵証明書 CER_{CP}
利用制御情状態データ (UCS) 166
SAM プログラム・ダウンロード・コンテナ $SD_1 \sim SDC_3$

【図 20】

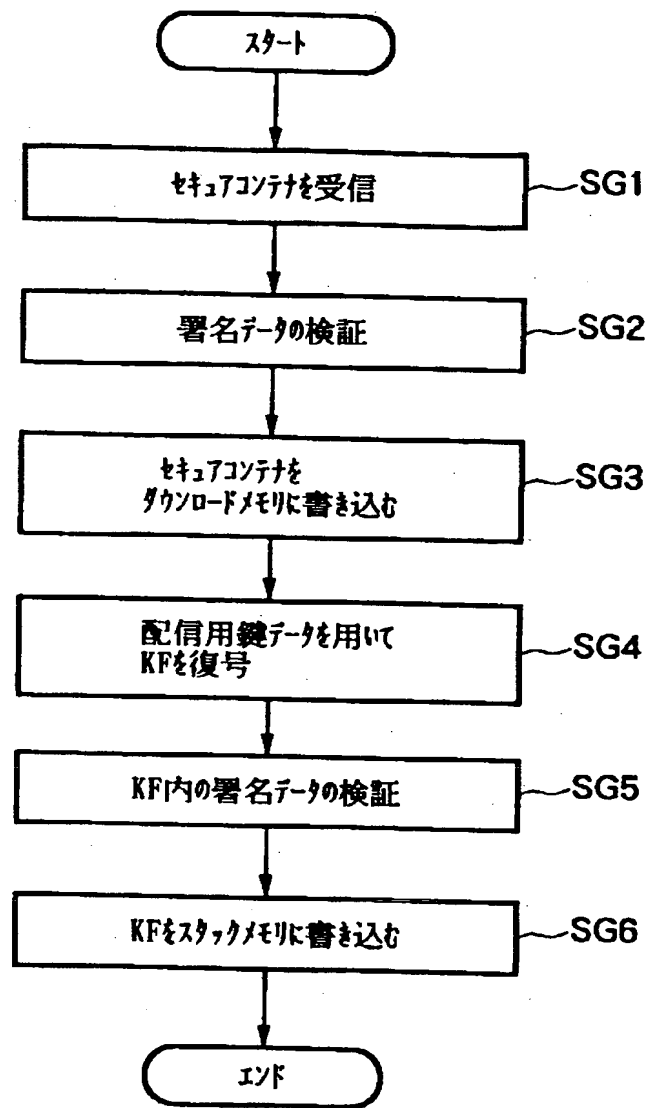


【図 21】

記憶部 192 に記憶されるデータ

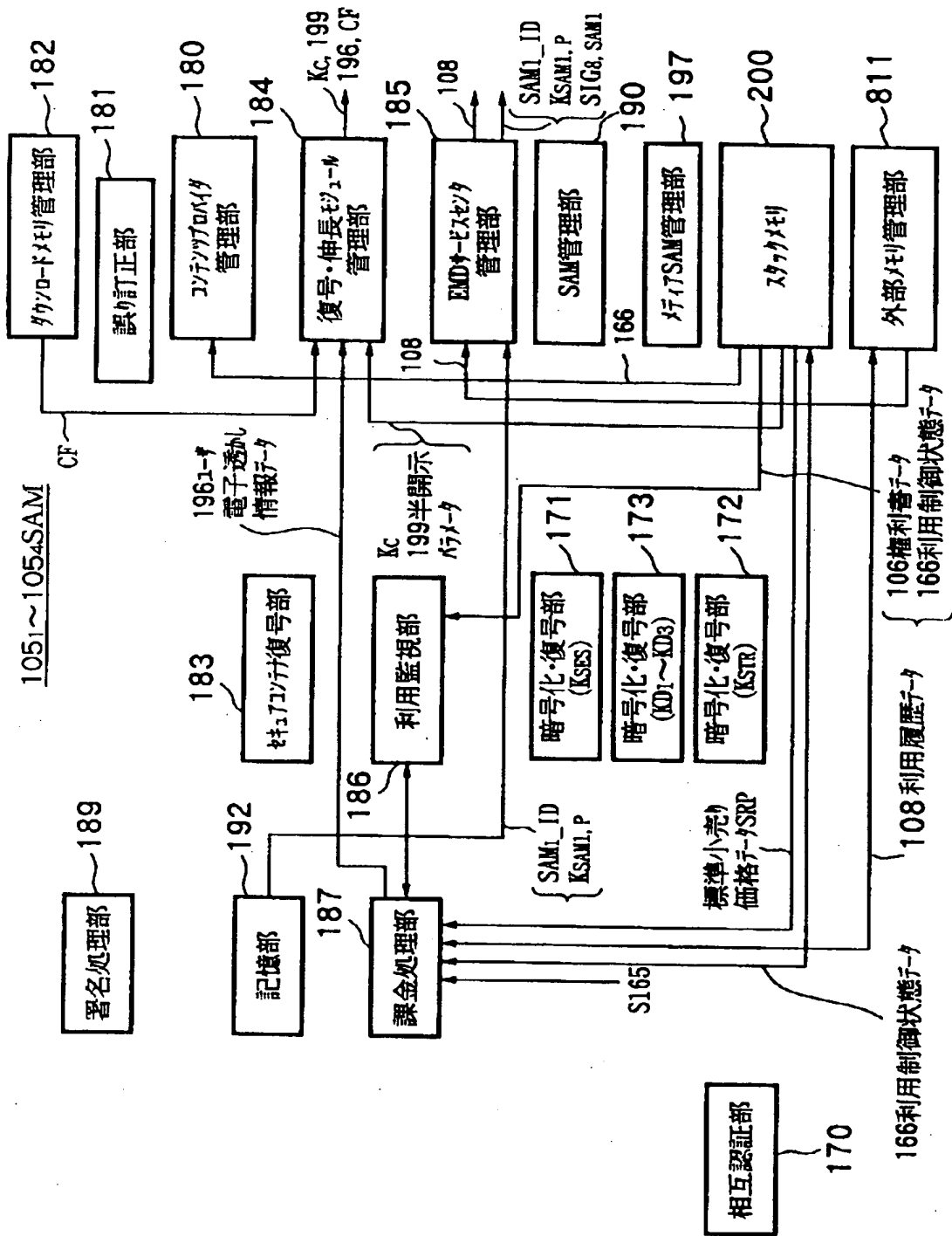


【図 22】

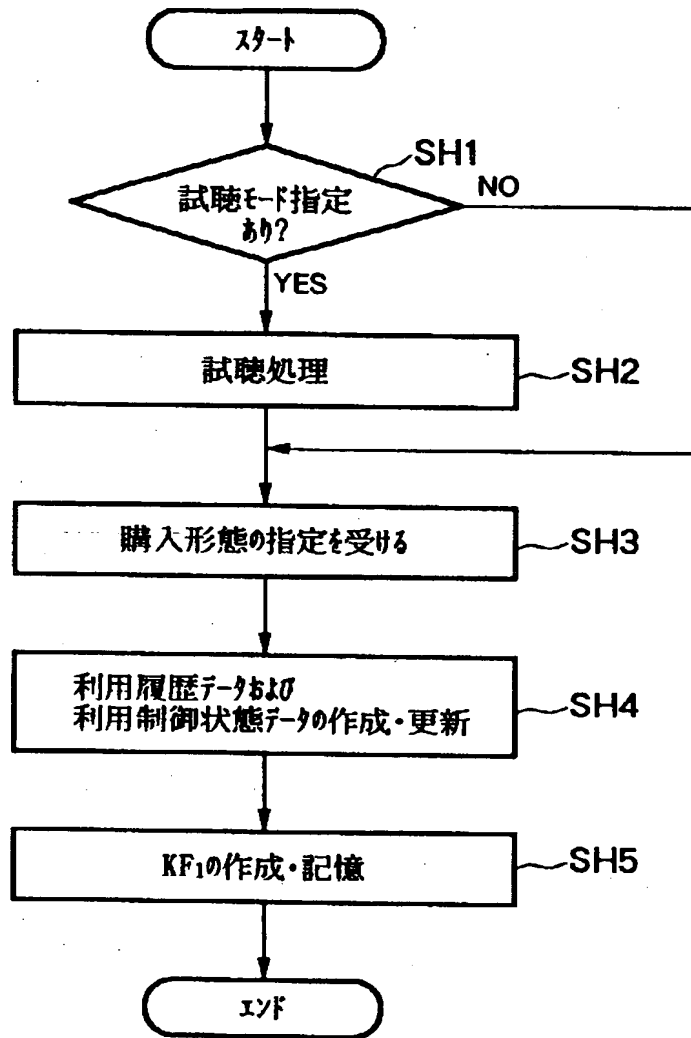


SAMにおけるKFの復号処理

【図 23】

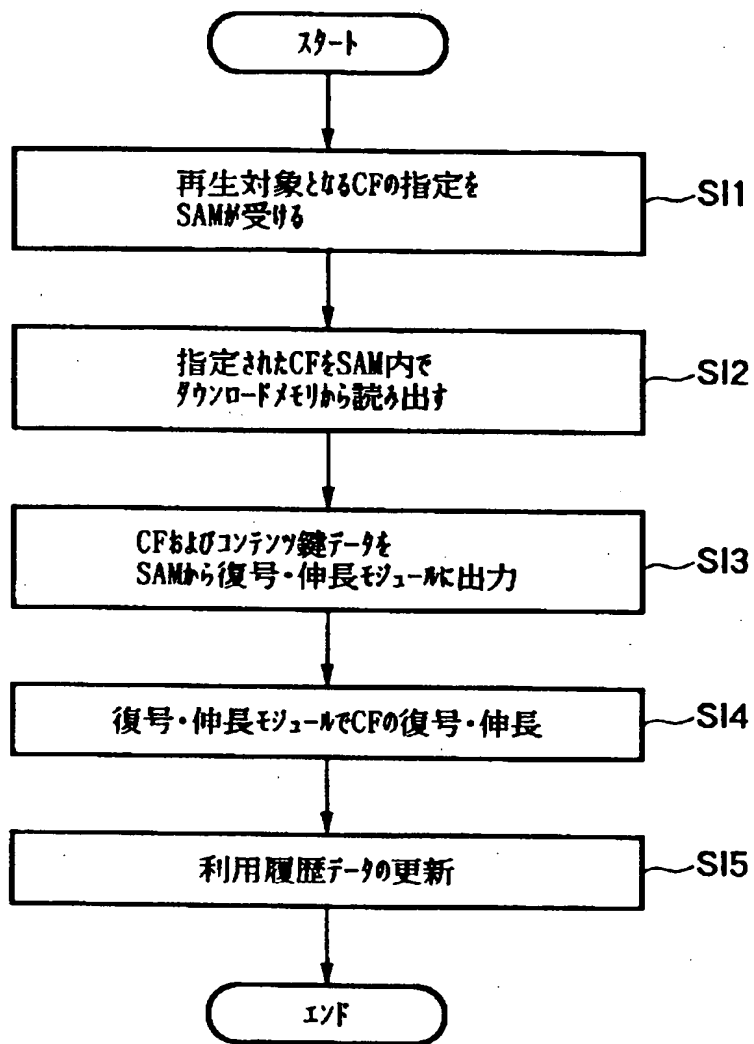


【図 24】



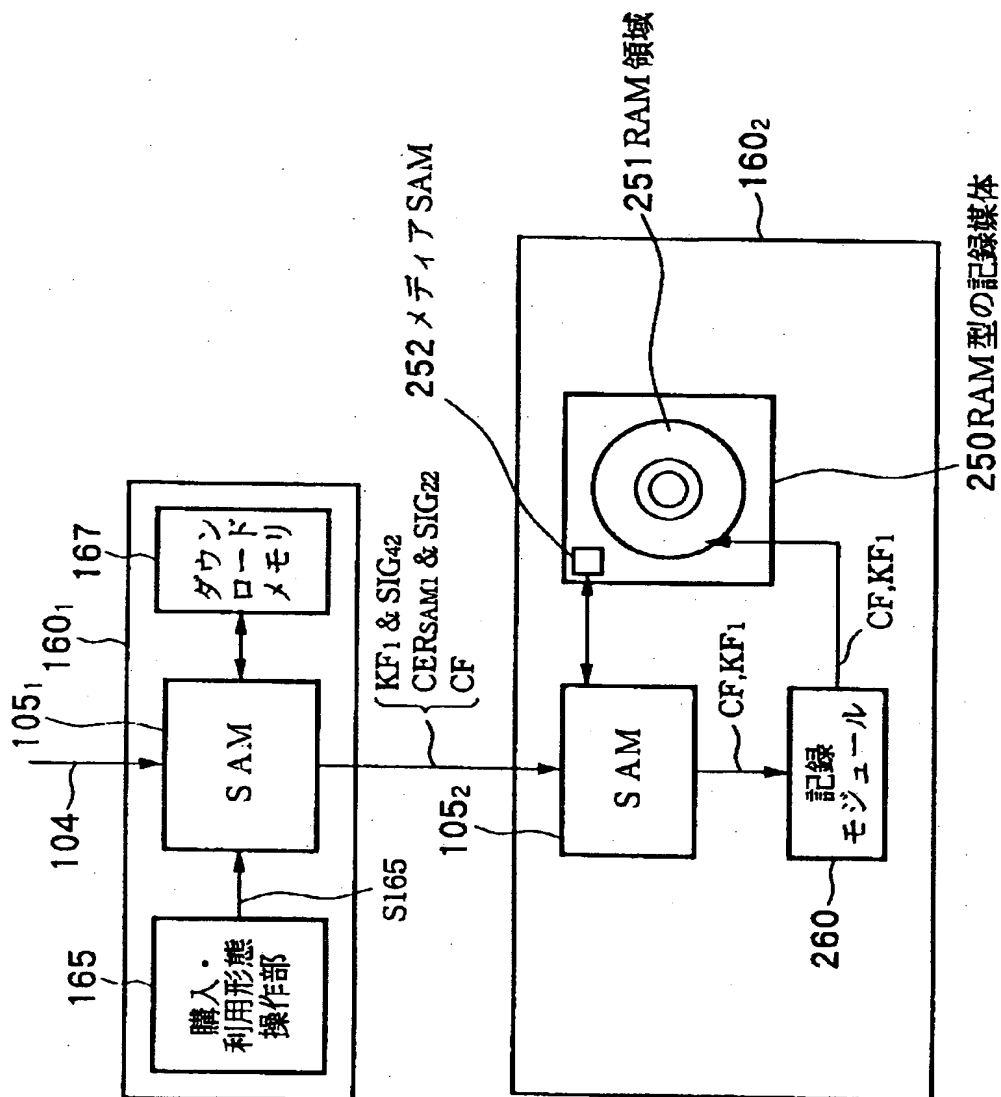
SAMにおけるセキアコンテナの購入形態決定処理

【図 25】

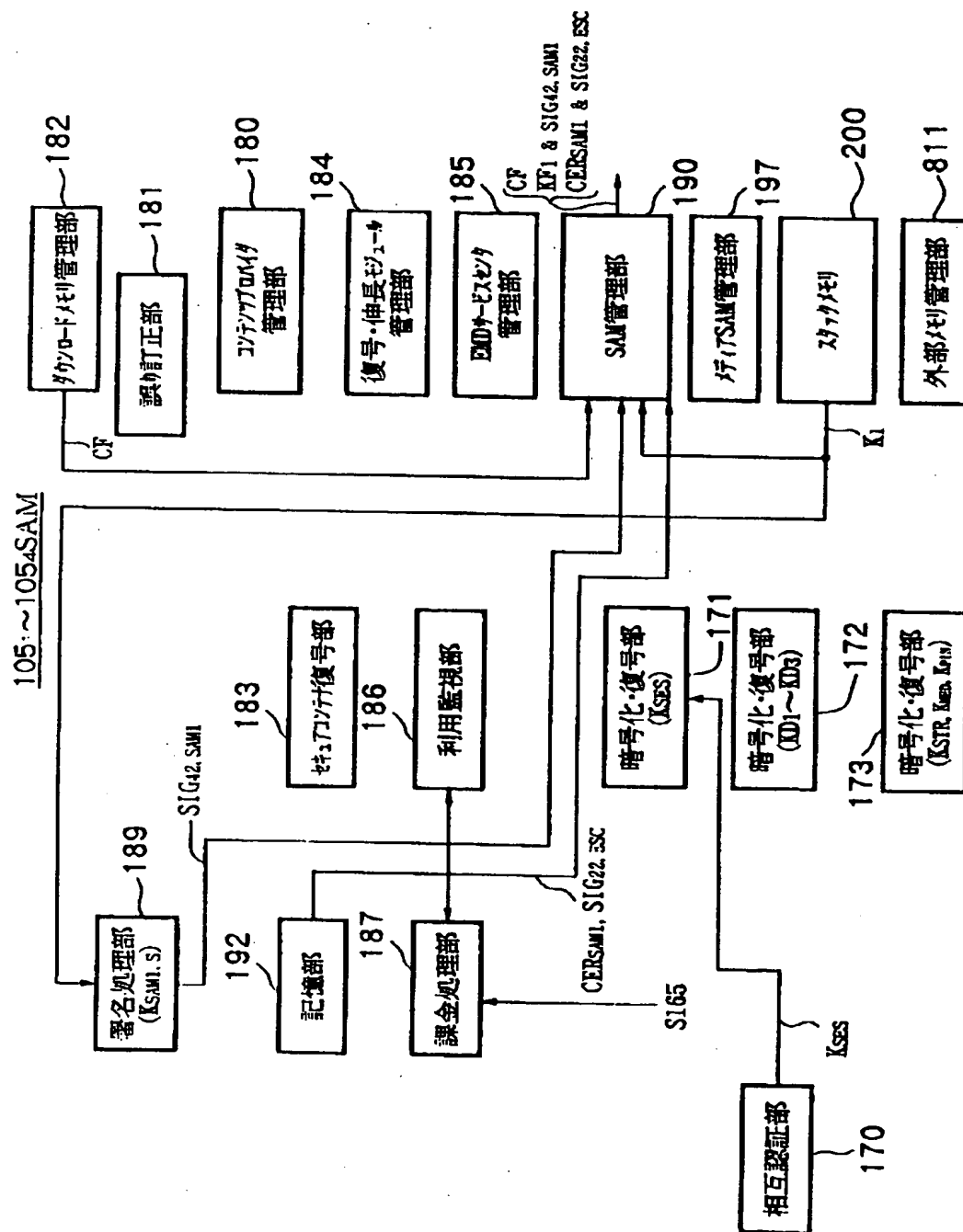


コンテンツデータの再生処理

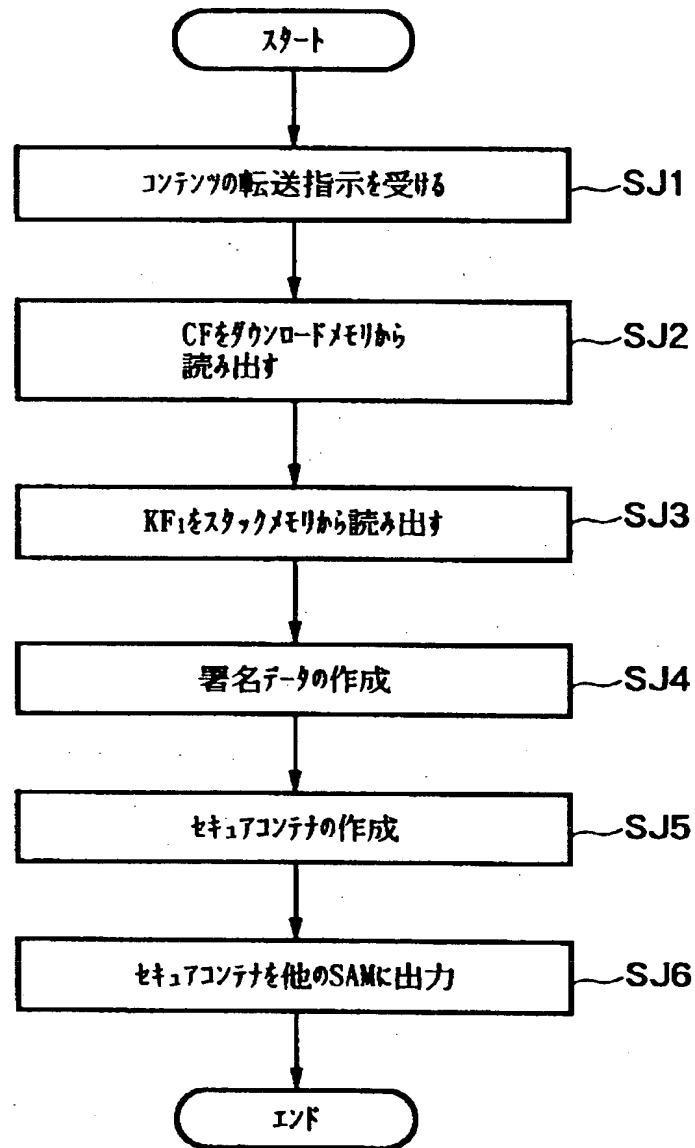
【図 26】



【图 2 7】

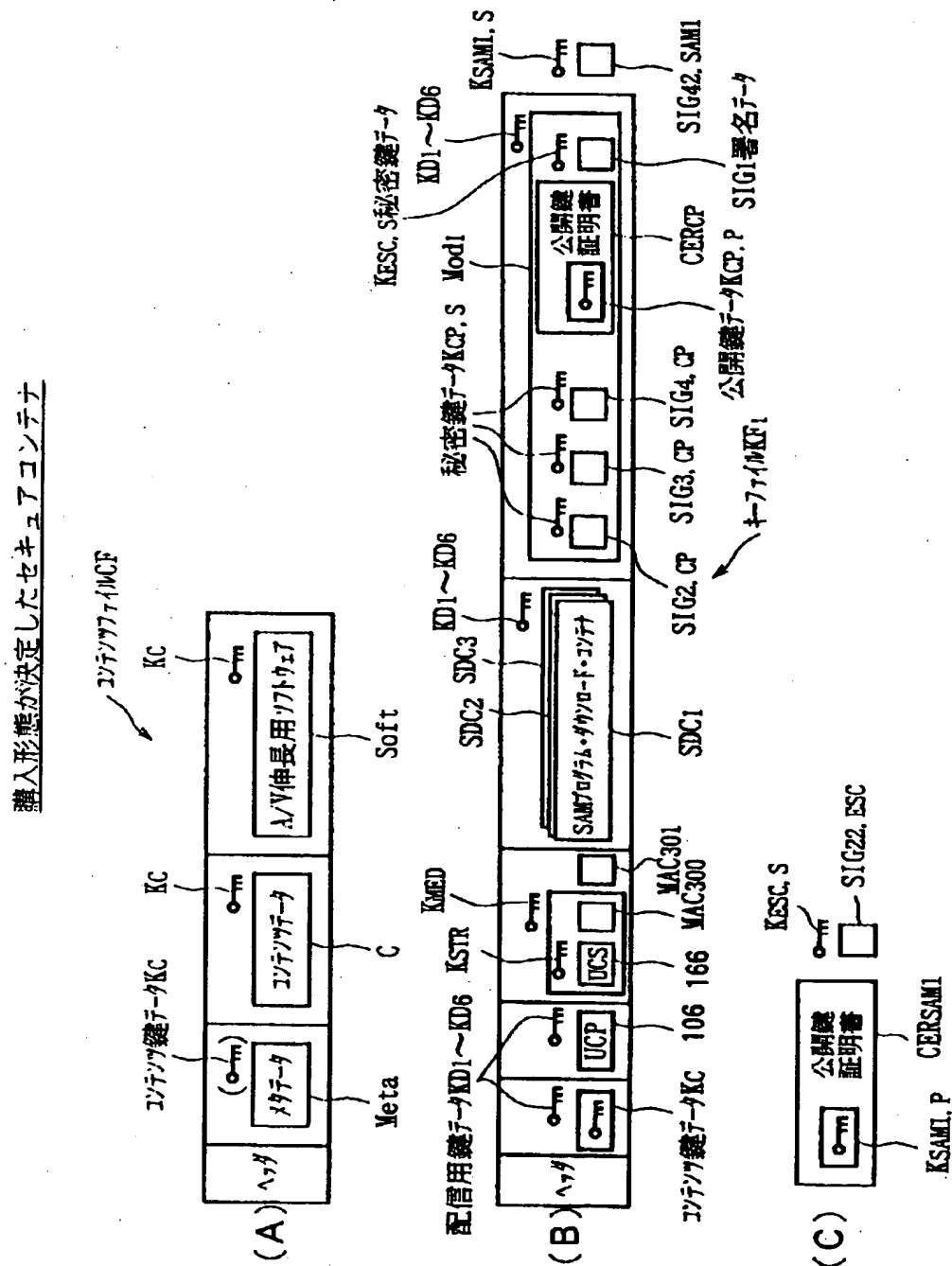


【図 28】

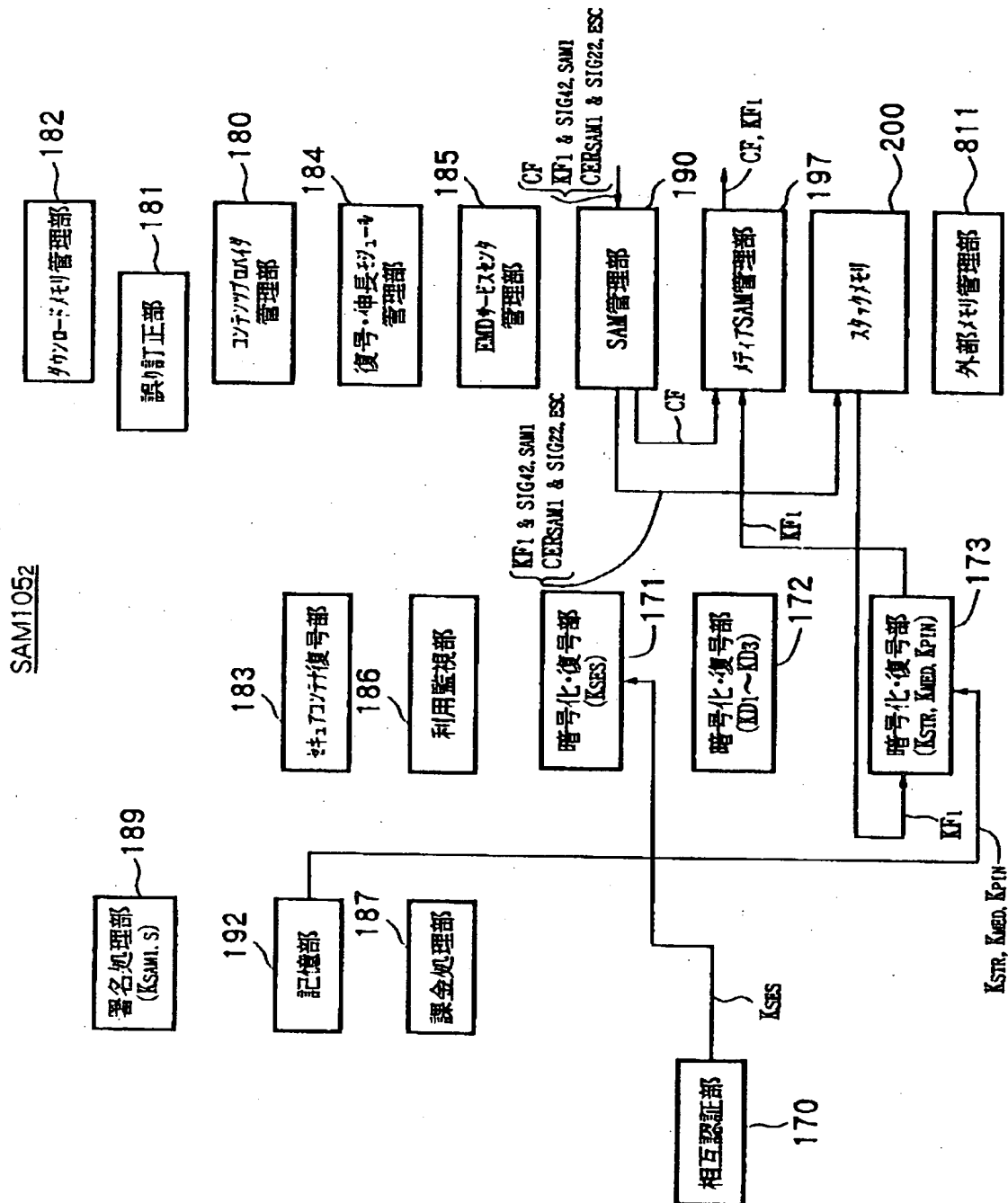


購入形態決定後のコンテンツを他のSAMに転送するSAMの処理

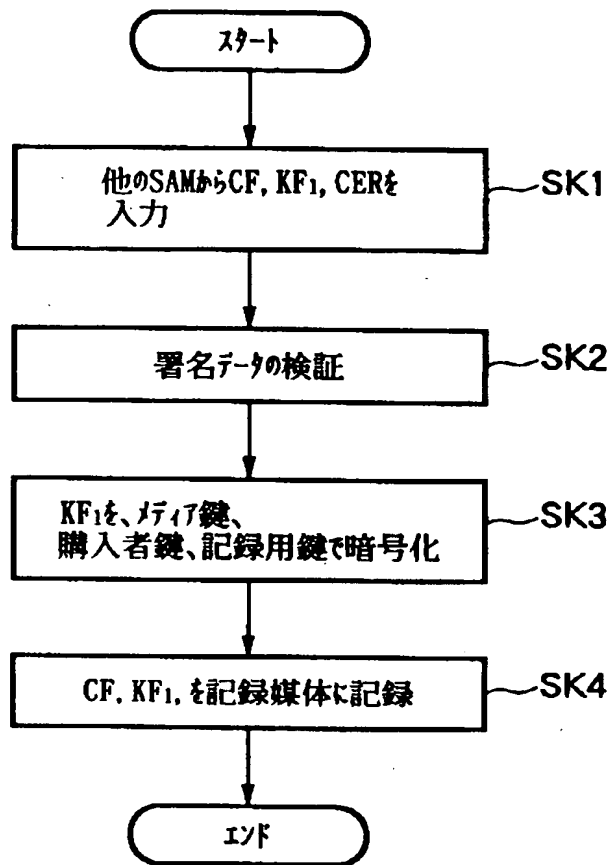
【図 29】



【図 30】

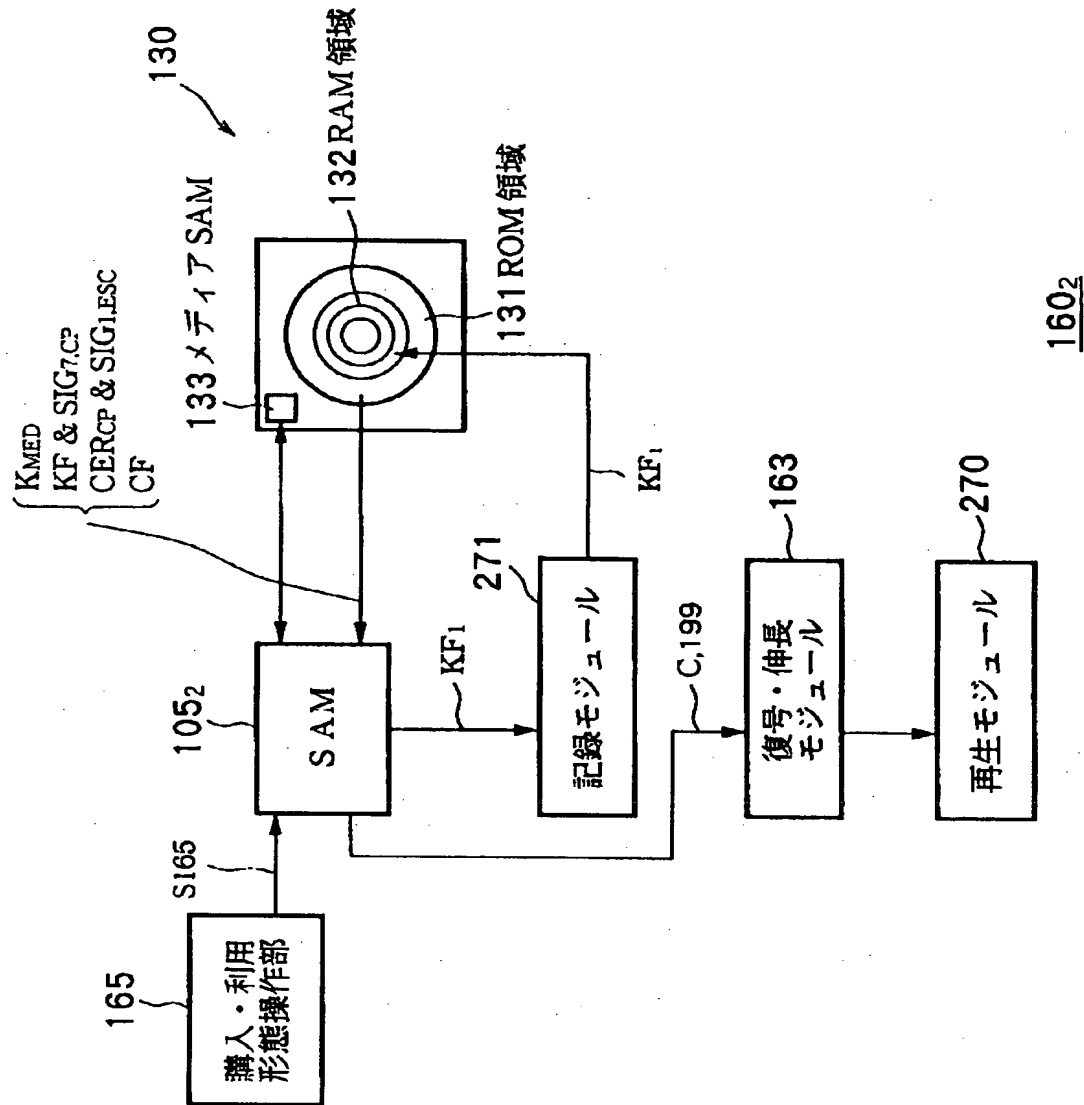


【図 3 1】



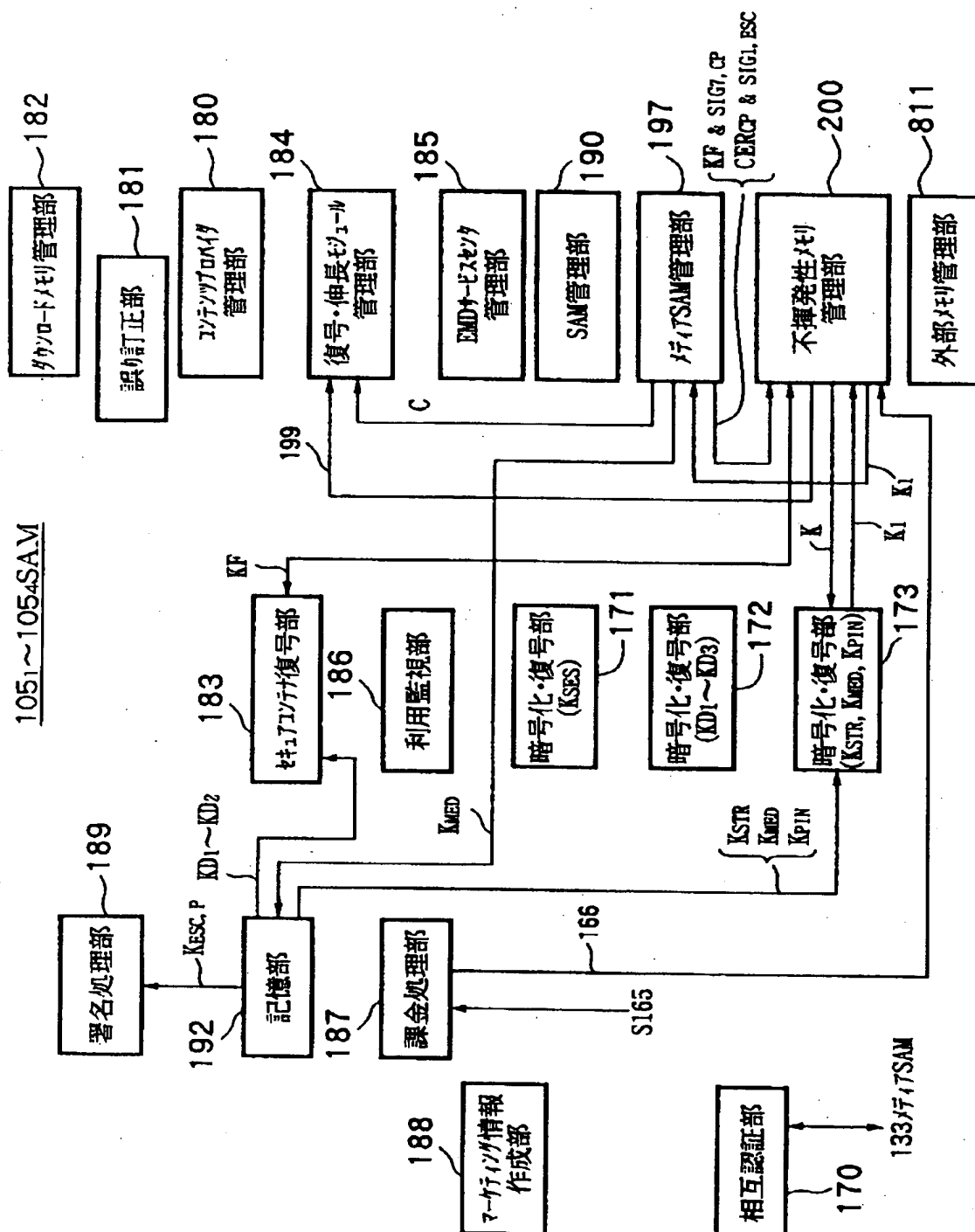
他のSAMから入力したCF等を記録媒体に書き込む際のSAMの処理

【図 3 2】

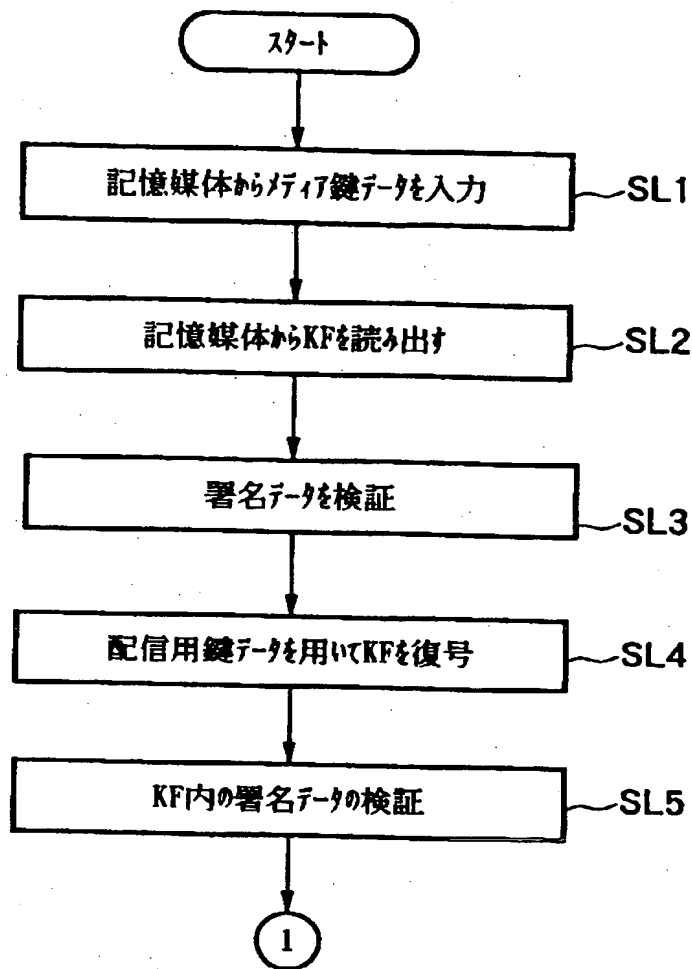


1602

【図 3 3】

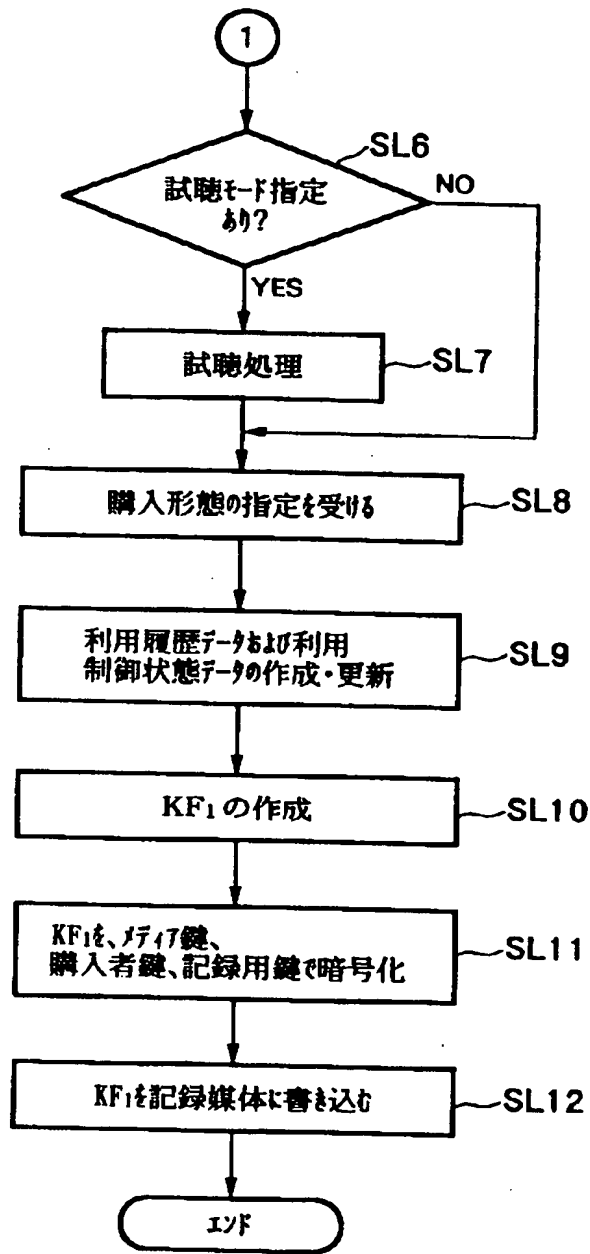


【図 34】



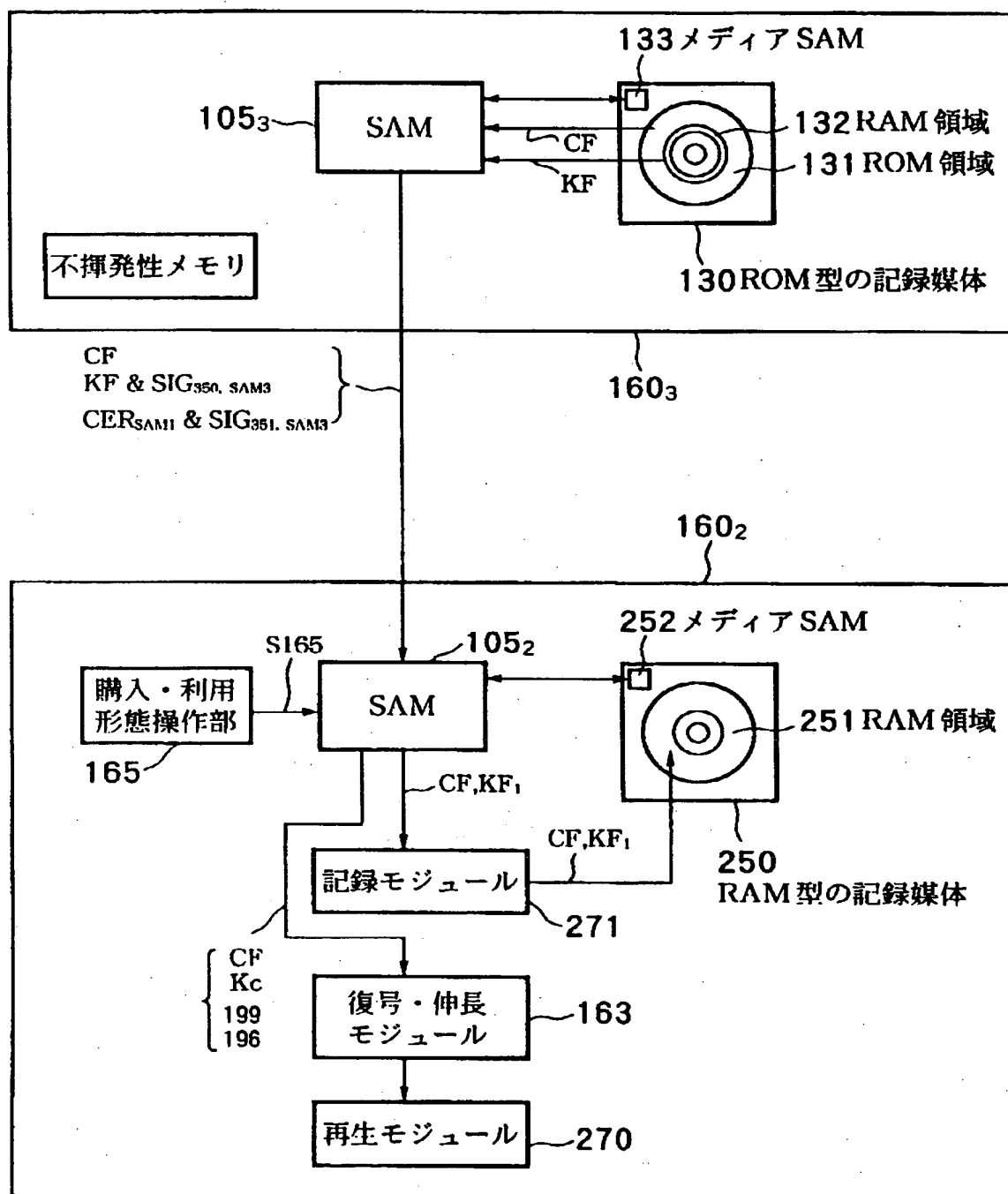
オンラインで配給されたコンテンツのSAMにおける購入形態決定処理

【図 35】

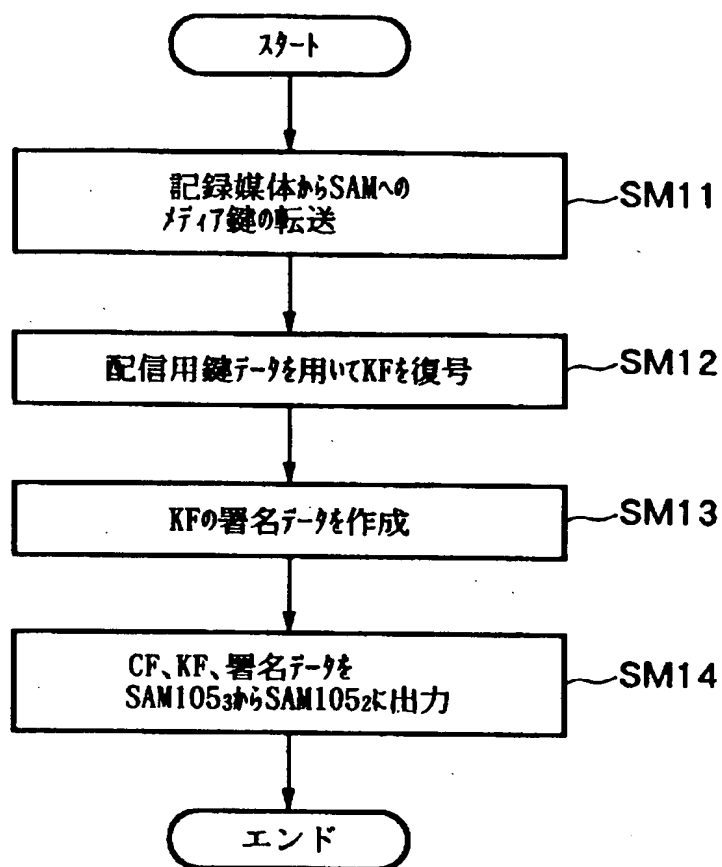


オンラインで配給されるコンテンツのSAMにおける購入形態決定処理

【図 36】

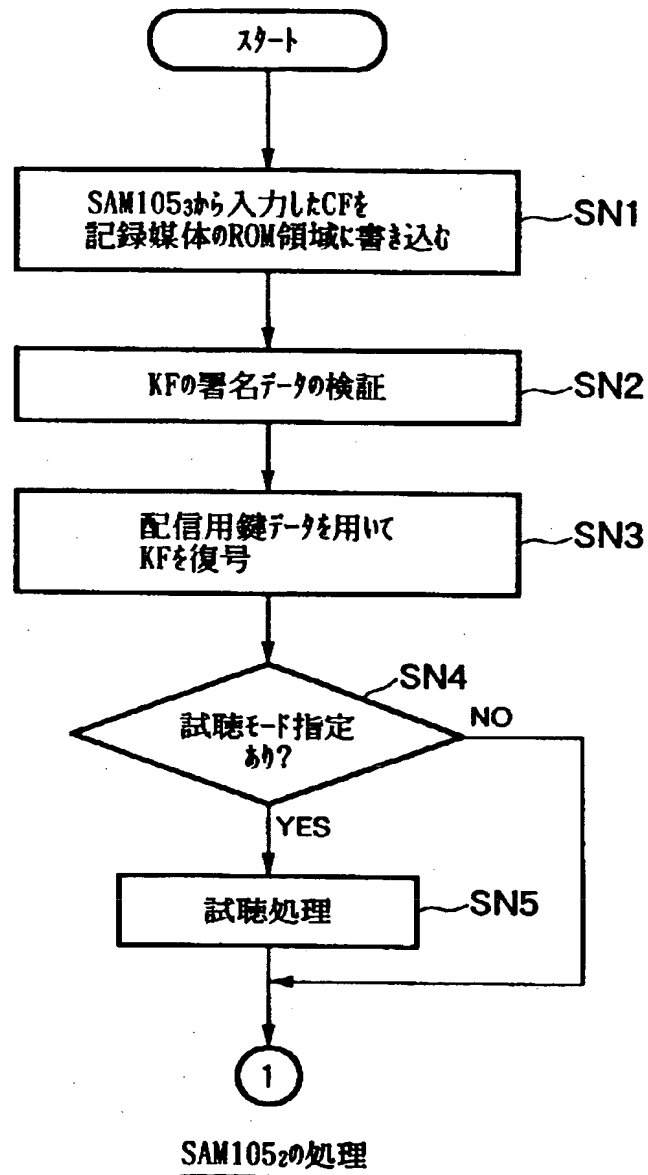


【図 37】

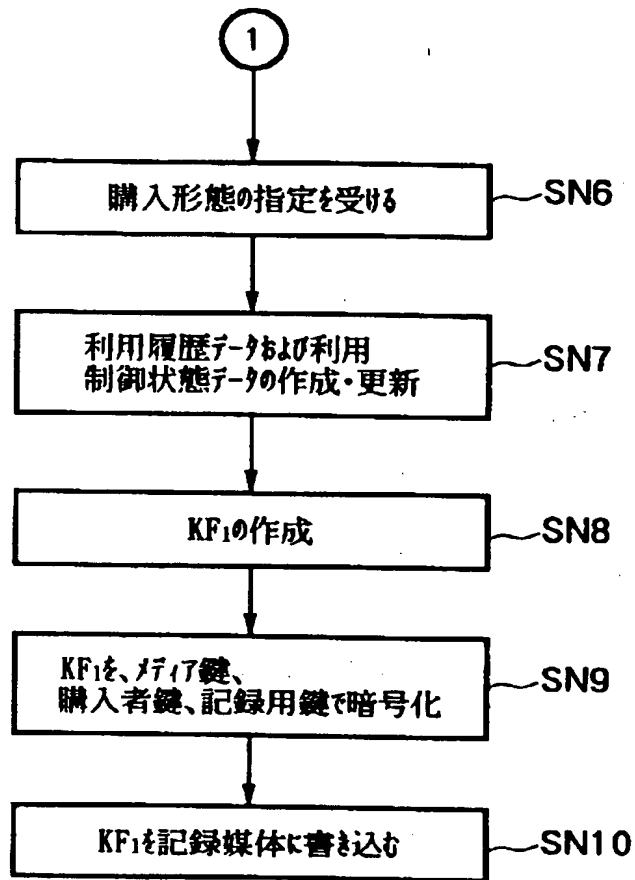


SAM1053の処理

【図38】

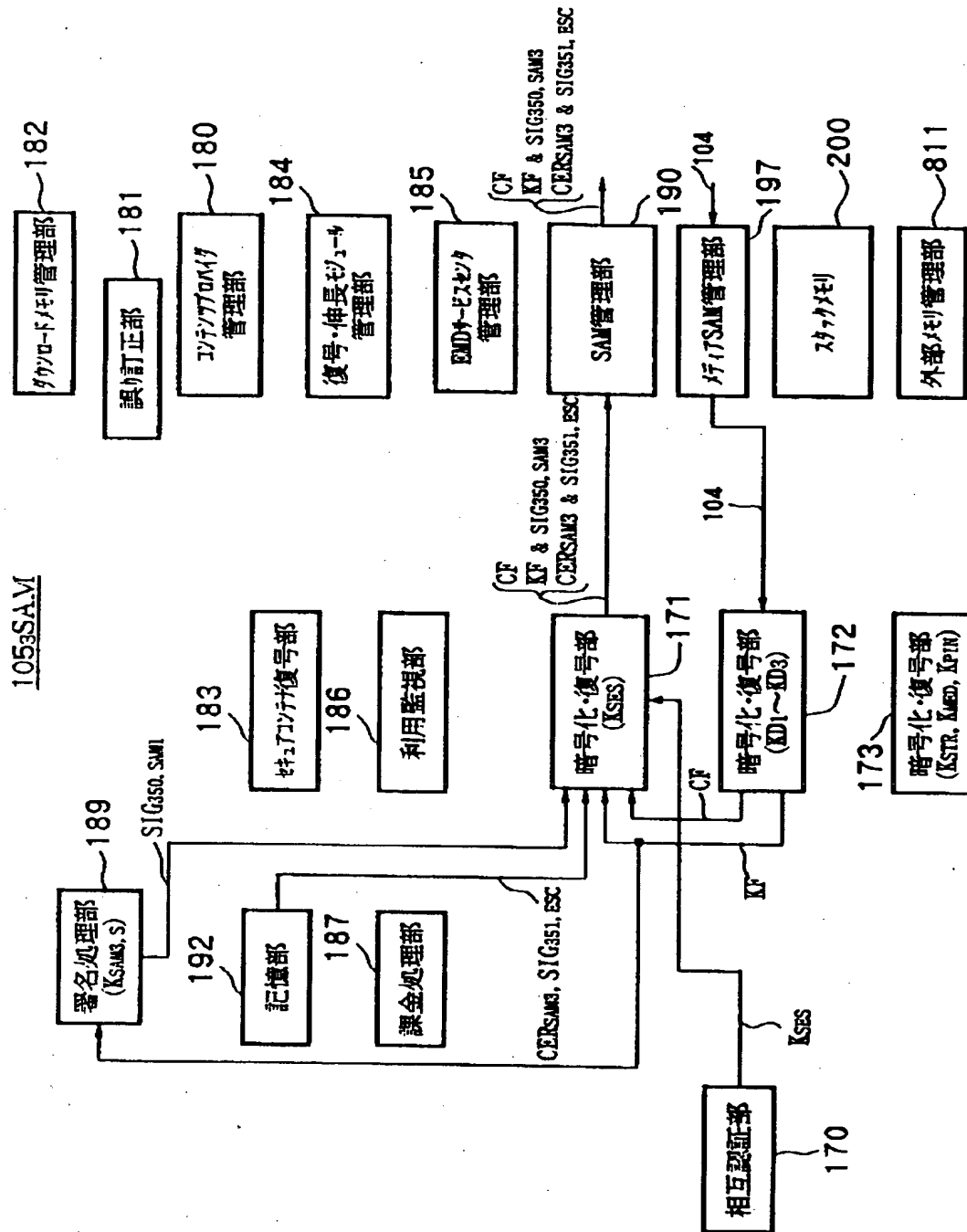


【図 39】

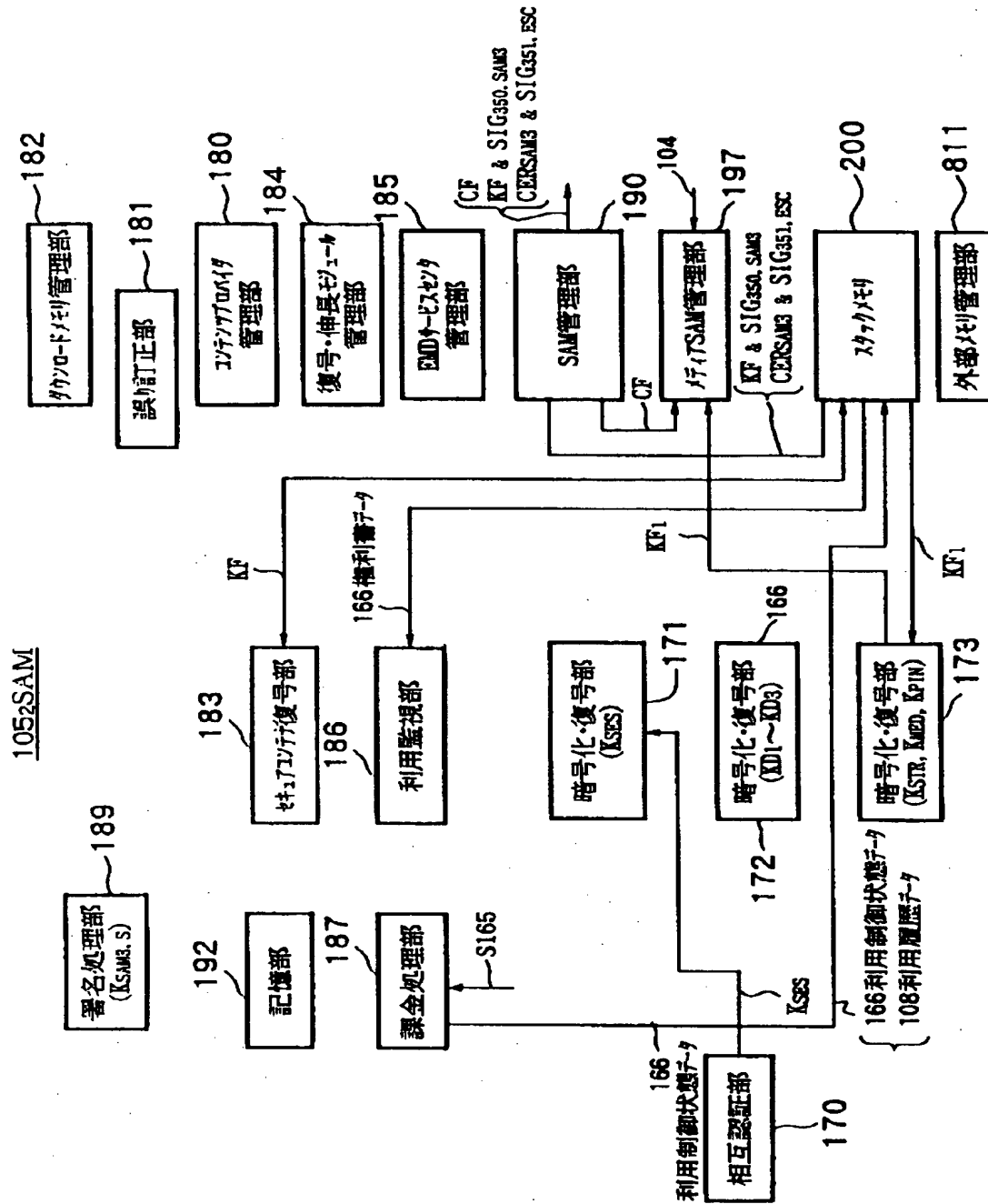


SAM1052の処理

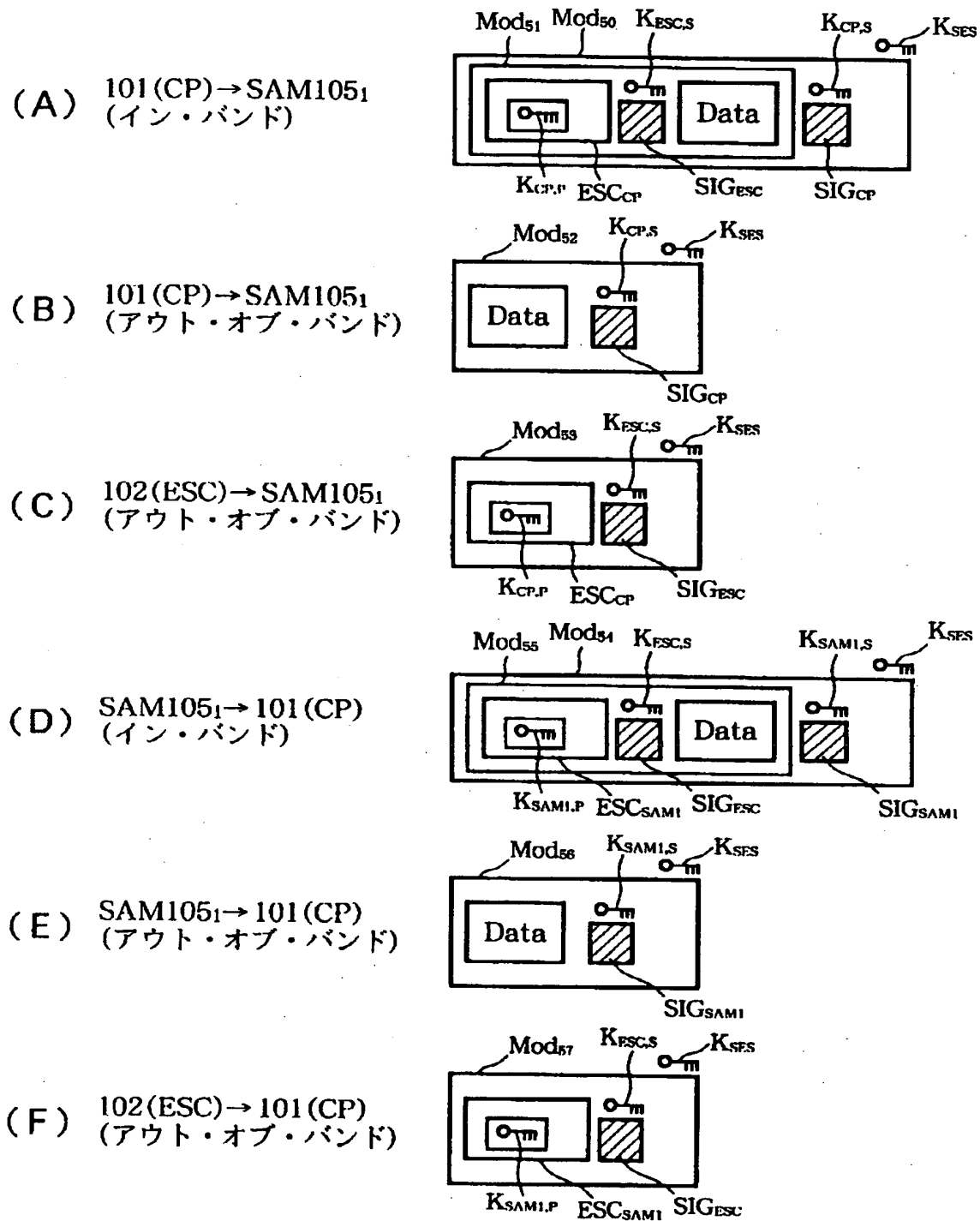
【図 40】



【図 41】

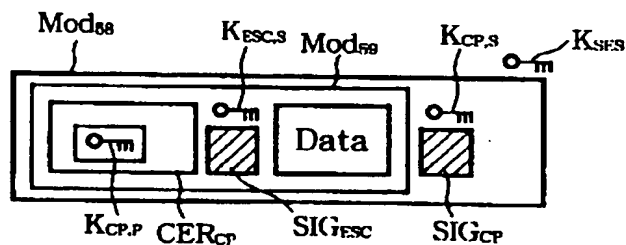


【図 4 2】

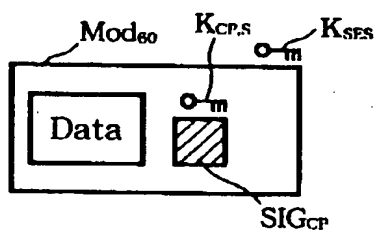


【図 43】

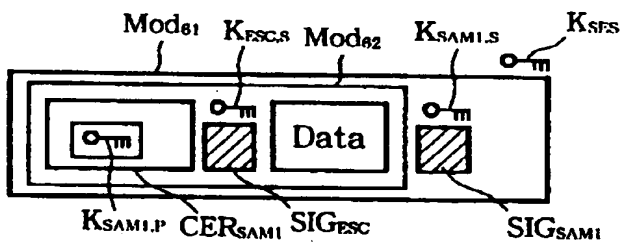
(G) 101(CP)→102(ESC)
(イン・バンド)



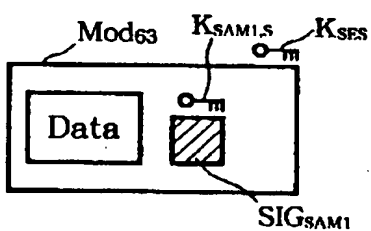
(H) 101(CP)→102(ESC)
(アウト・オブ・バンド)



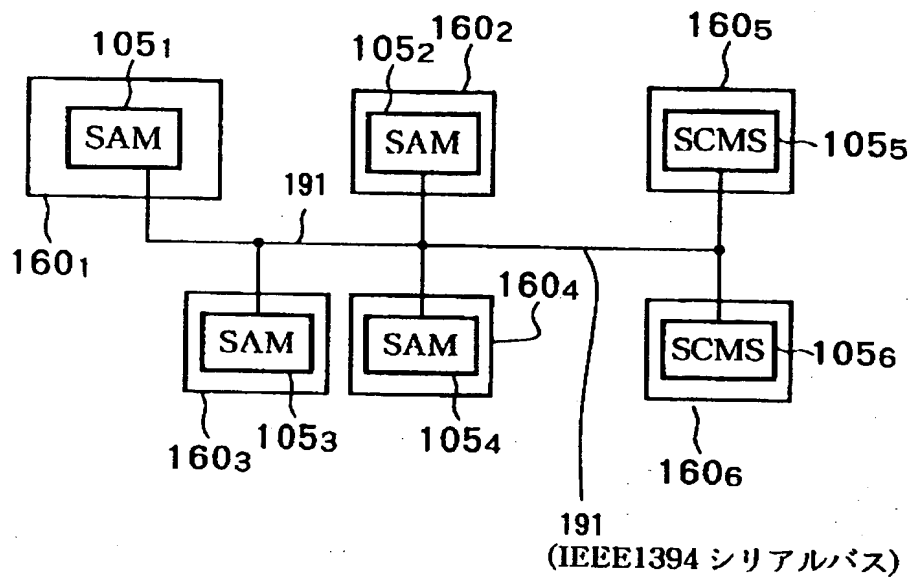
(I) SAM1051→102(ESC)
(イン・バンド)



(J) SAM1051→102(ESC)
(アウト・オブ・バンド)



【図 4 4】

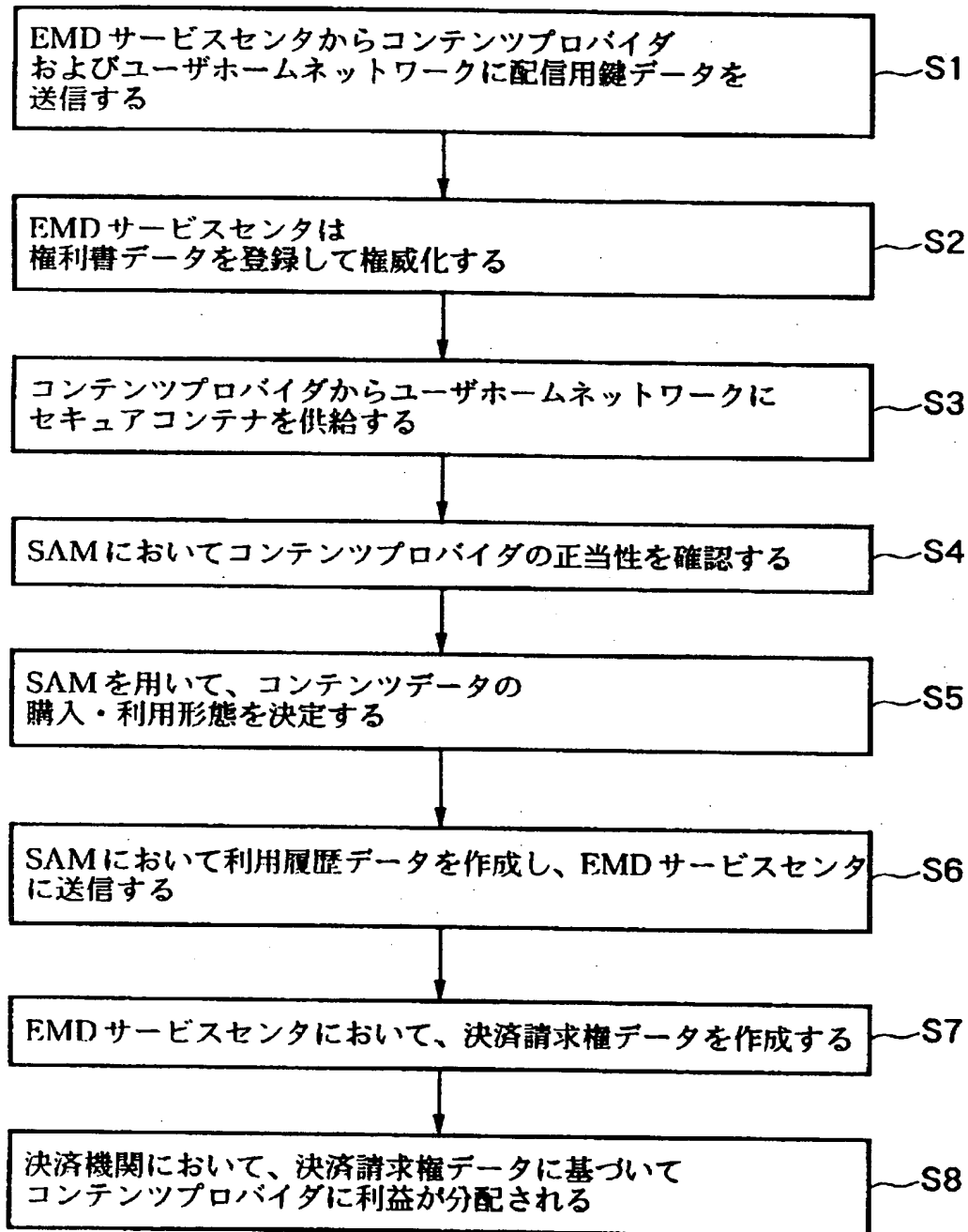


【図 4 5】

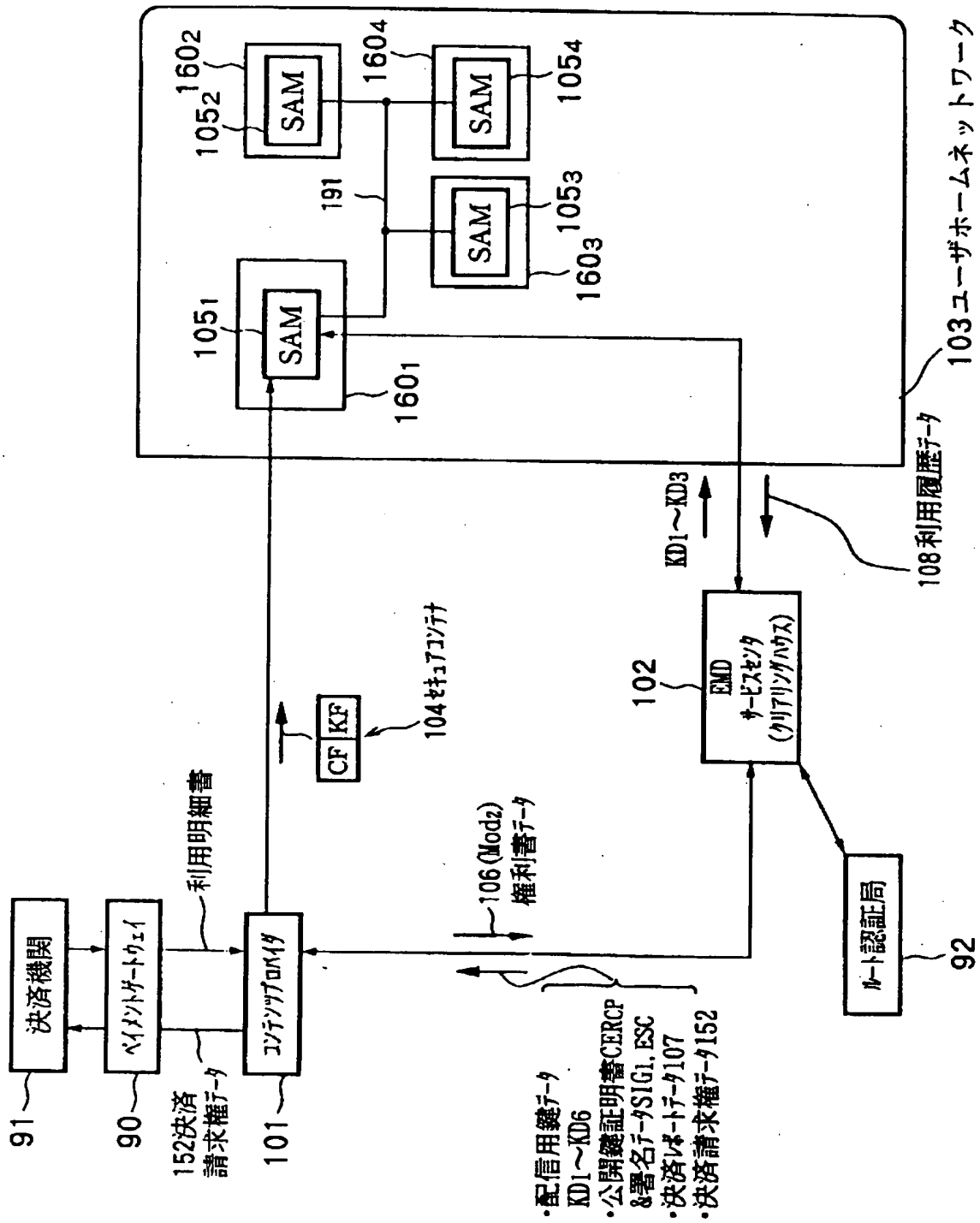
リストを発行したSAMのSAM_ID(Issure_SAM)
SAM登録リストの有効期限
SAM登録数
SAMの接続リスト(SAM_ID)
SAMの決済機能 有/無(Settlement Function)
Revocation_Flag そのSAMがリボークされているか。
各々のSAMの公開鍵
ESC 秘密鍵による署名データ
<div> <div>ハッシュ関数</div> <div> <div>リストを発行したSAMのSAM_ID(Issure_SAM)</div> <div>Registration Listの有効期限</div> <div>SAM登録数</div> <div>SAMの接続リスト(SAM_ID)</div> <div>SAMの決済機能 有/無(Settlement Function)</div> <div>Revocation_Flag そのSAMがリボークされているか。</div> <div>各々のSAMの公開鍵</div> </div> </div>

SAM登録リスト

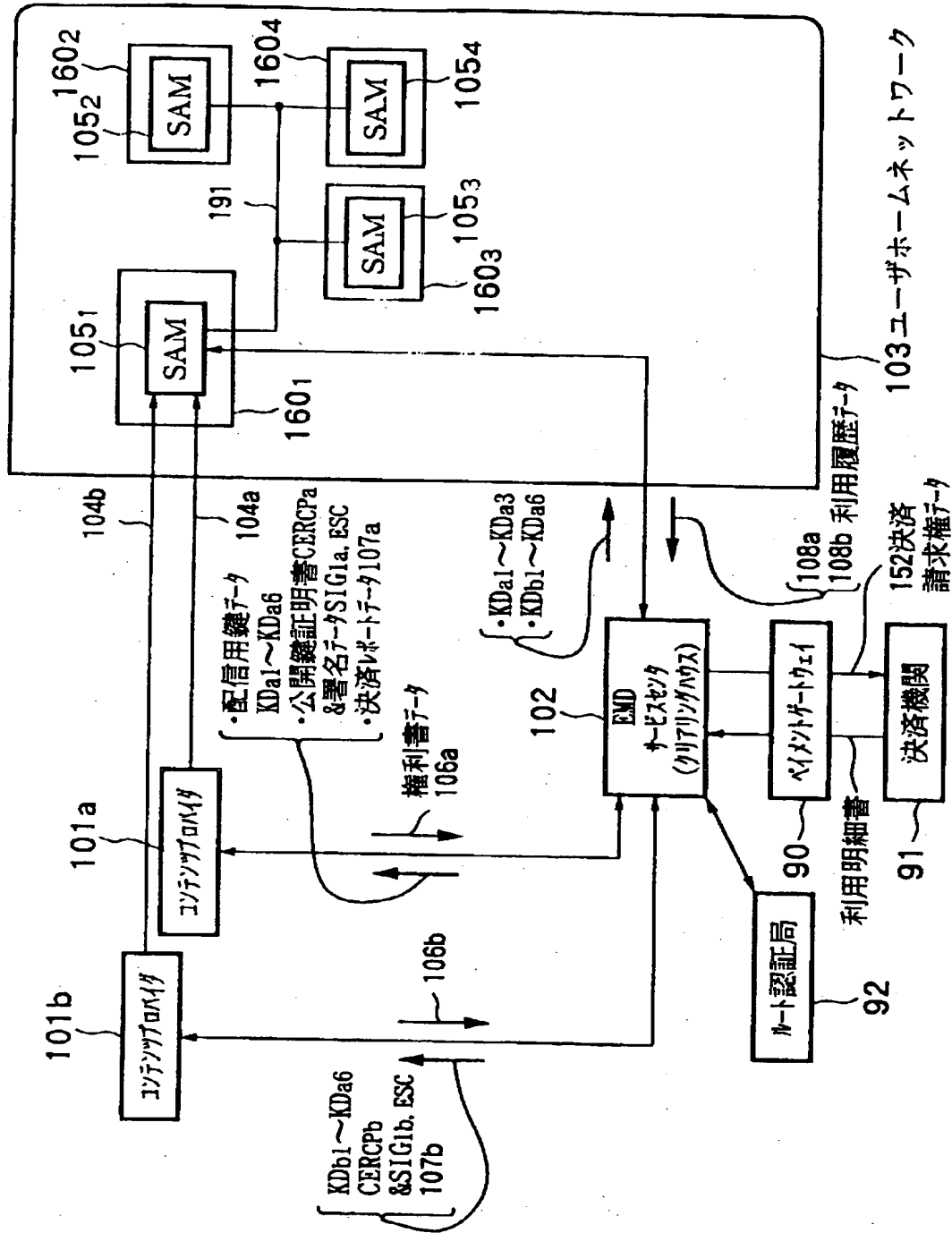
【図 4 6】



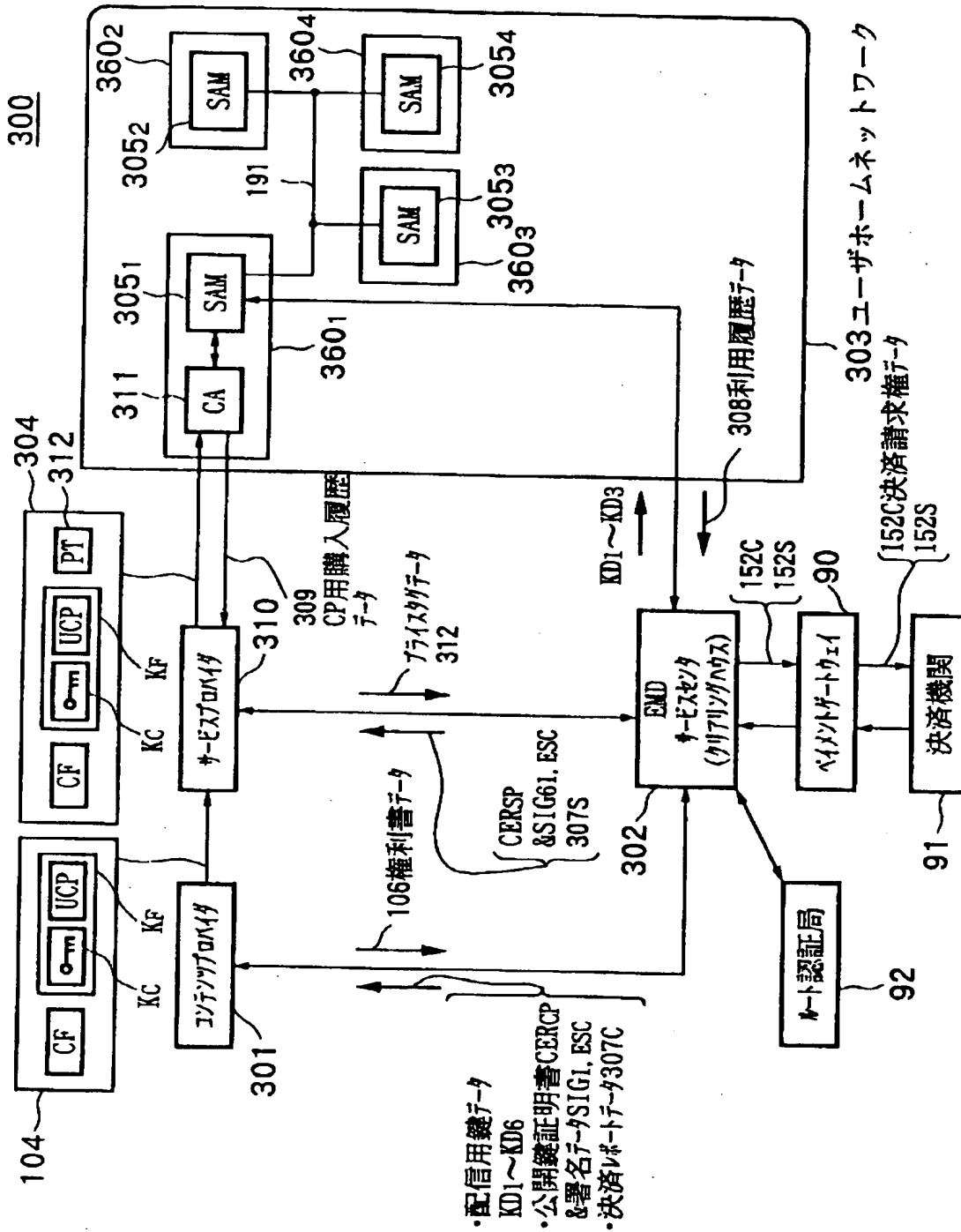
【図 47】



【図48】

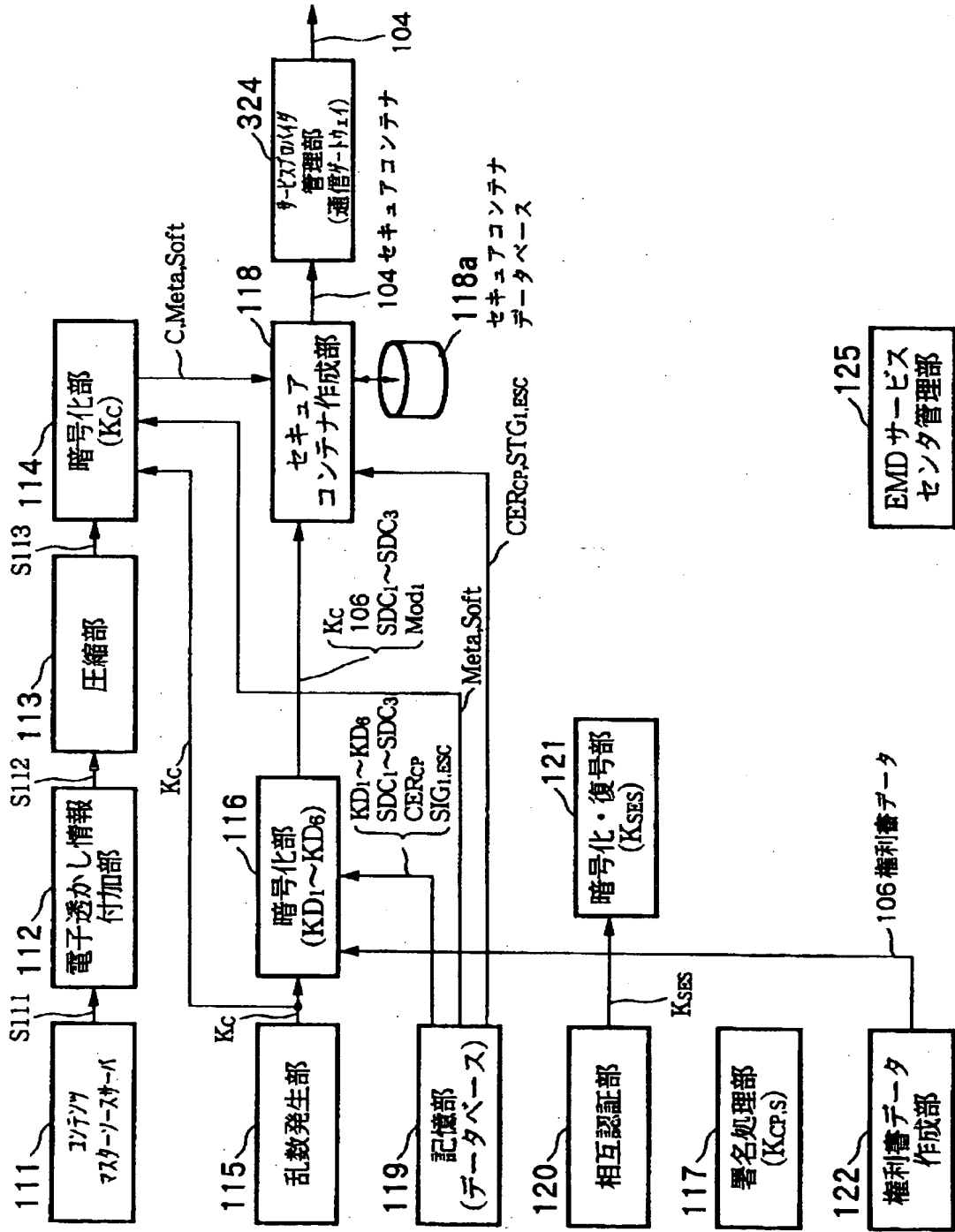


【図 49】

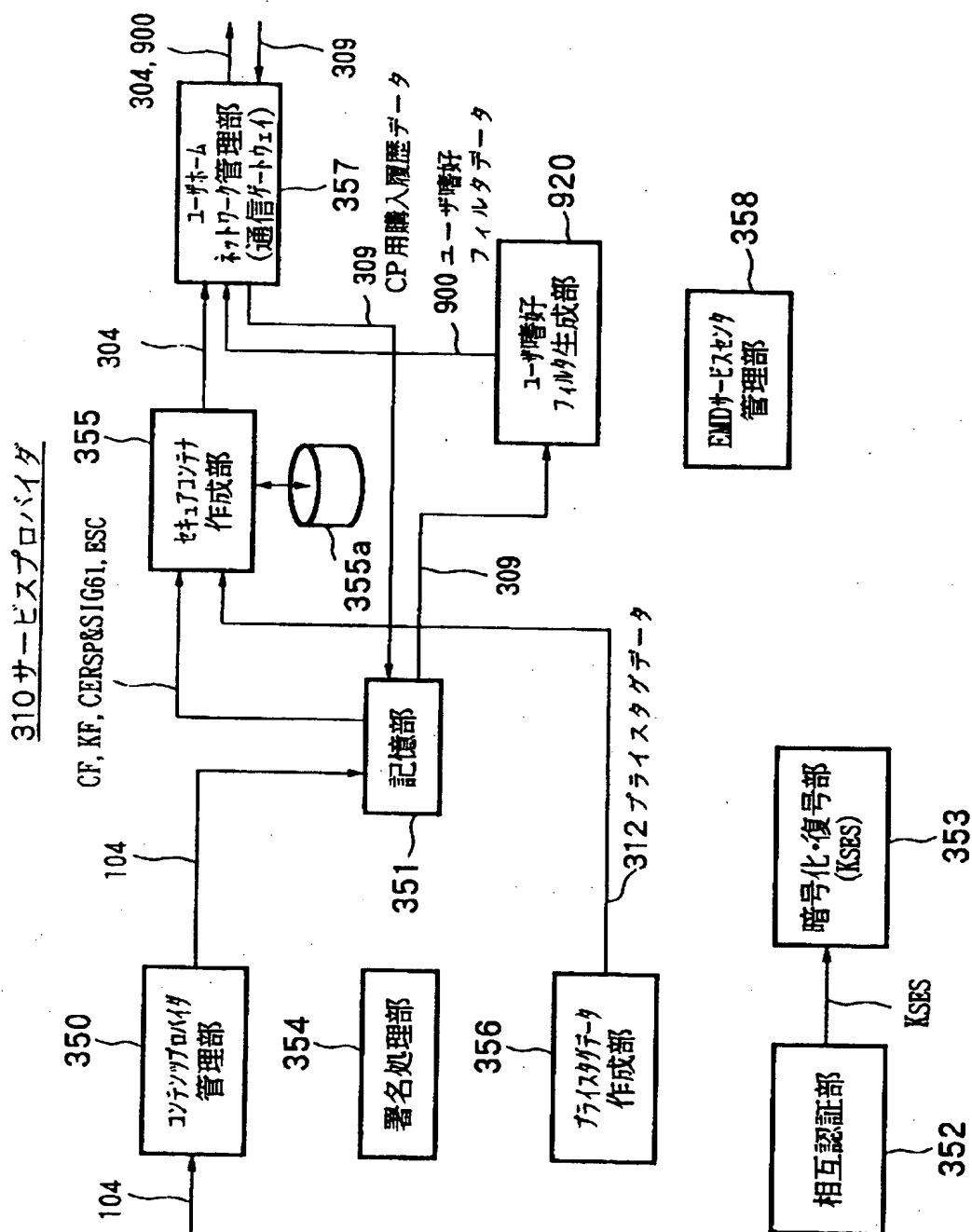


【図50】

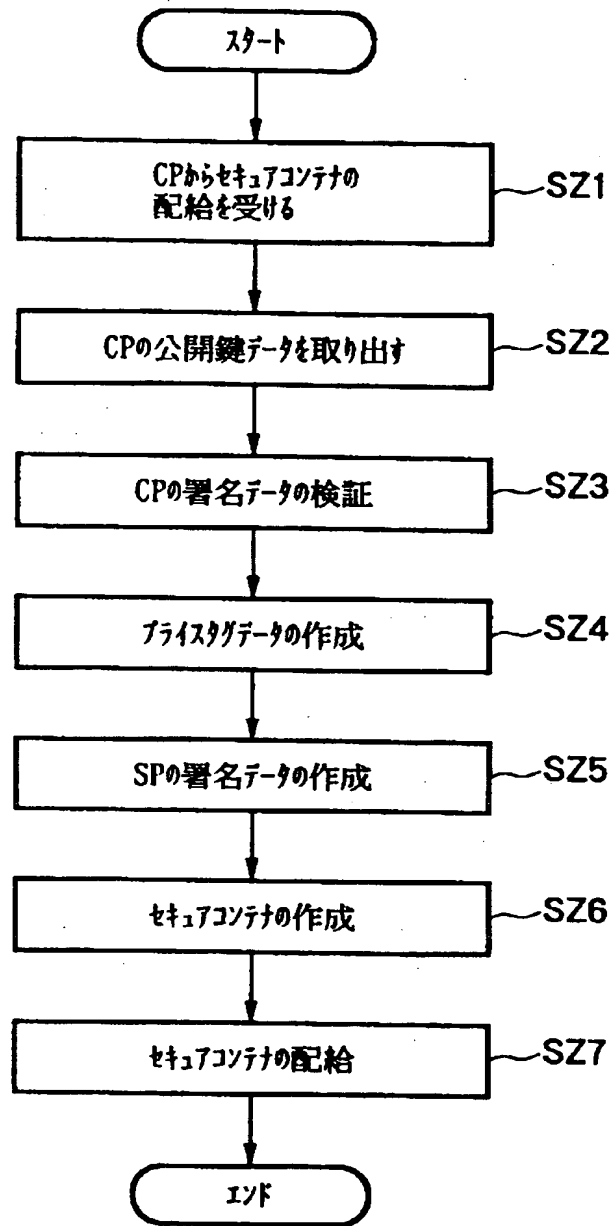
301 コンテンツプロバイダ



【图 5 1】

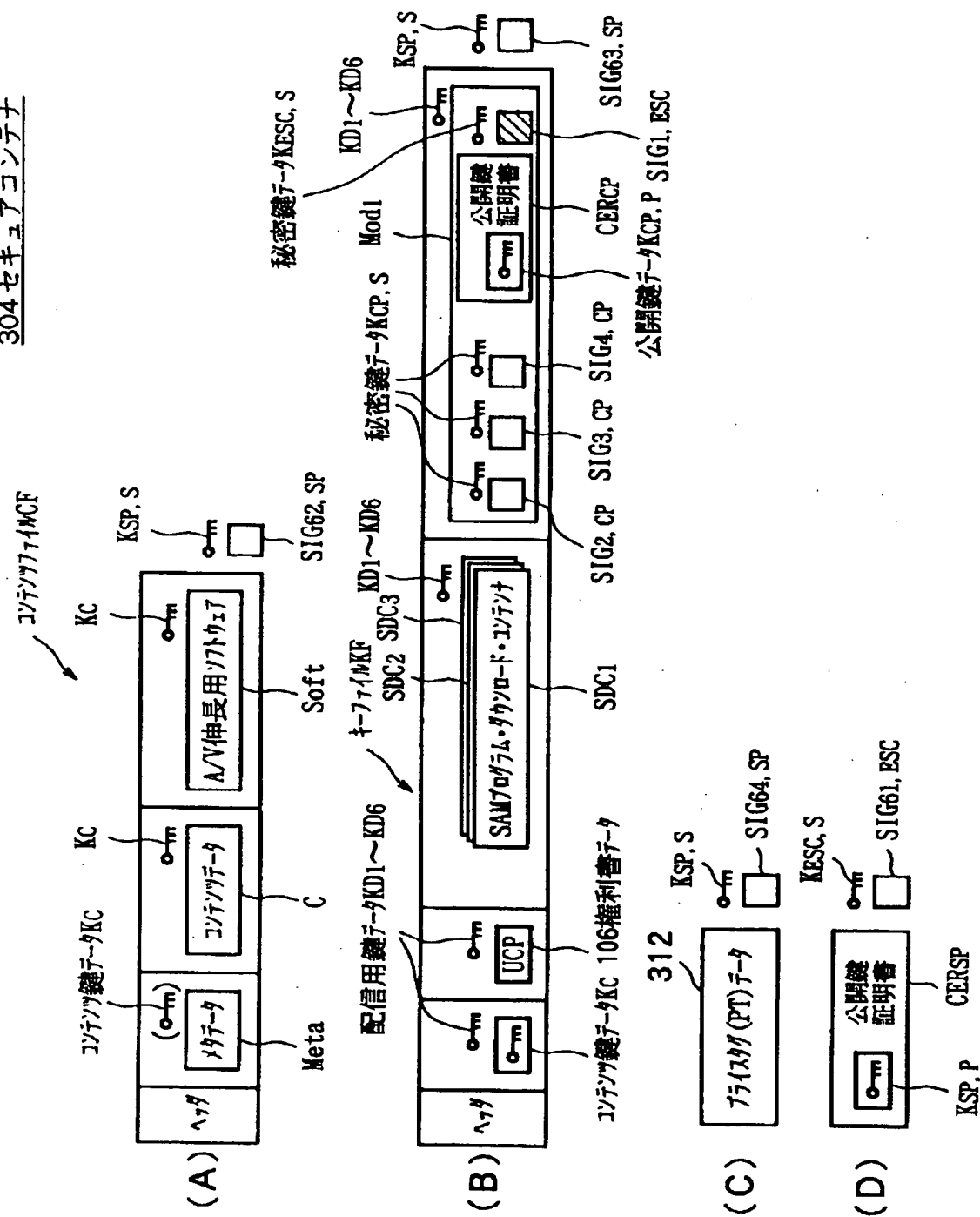


【図 52】



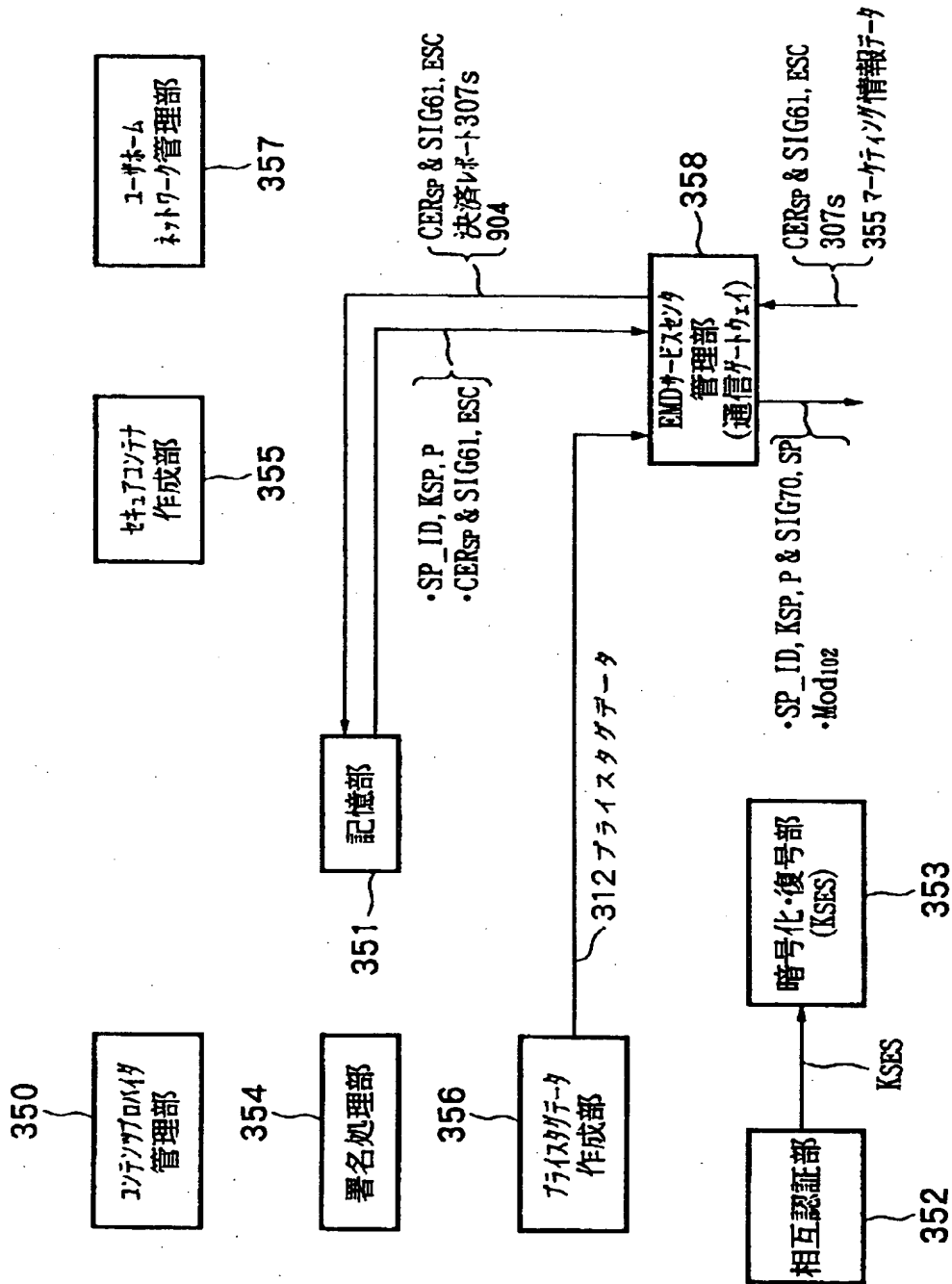
【図 53】

304 セキュアコンテナ

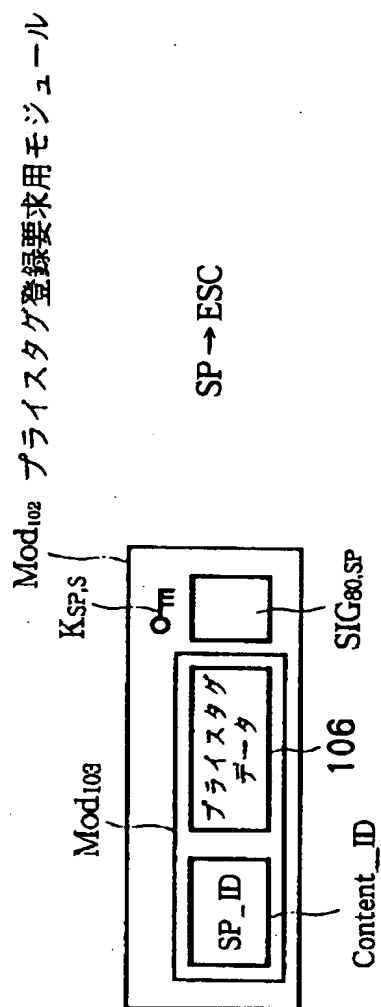


【図 54】

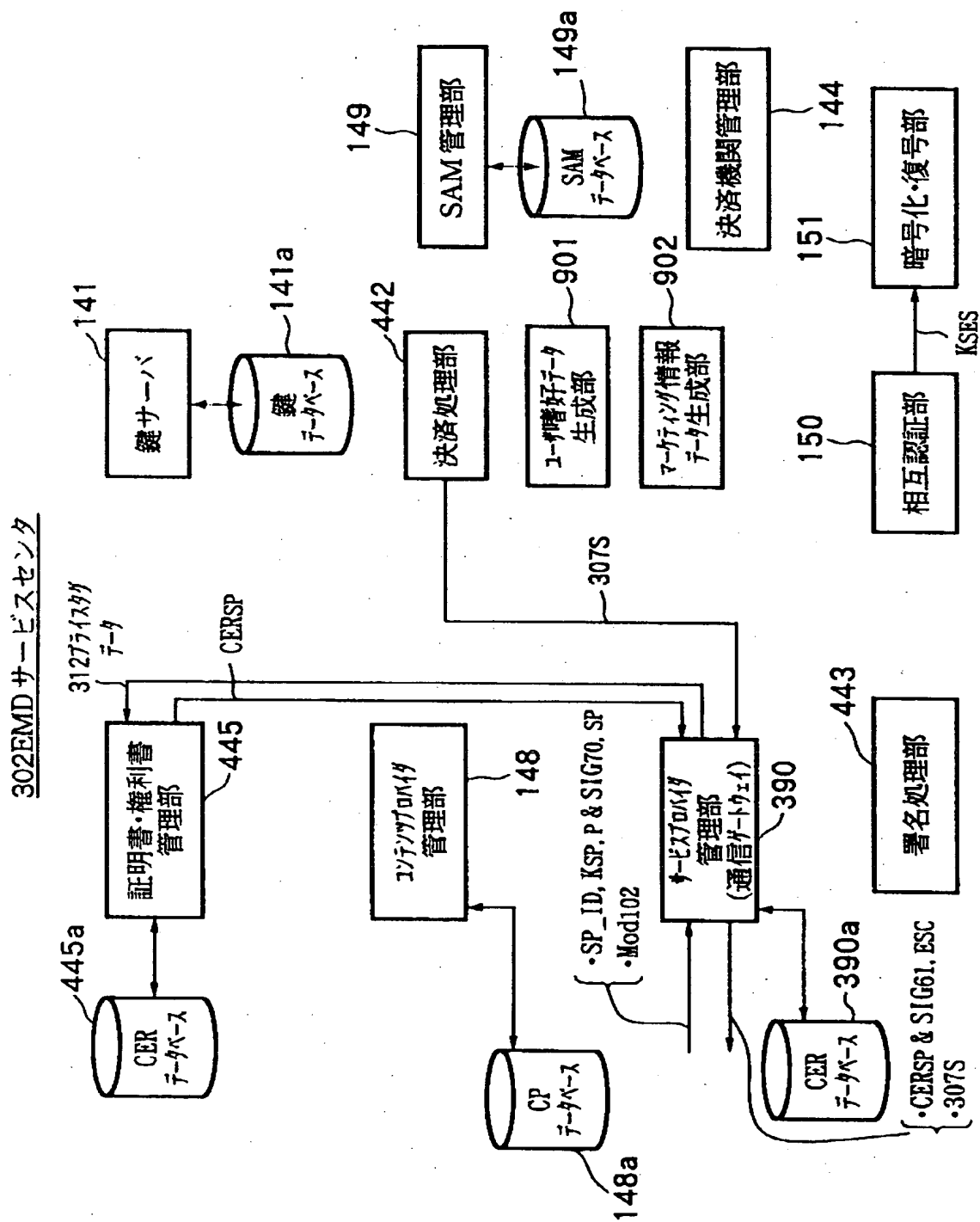
310 サービスプロバイダ



【図 55】

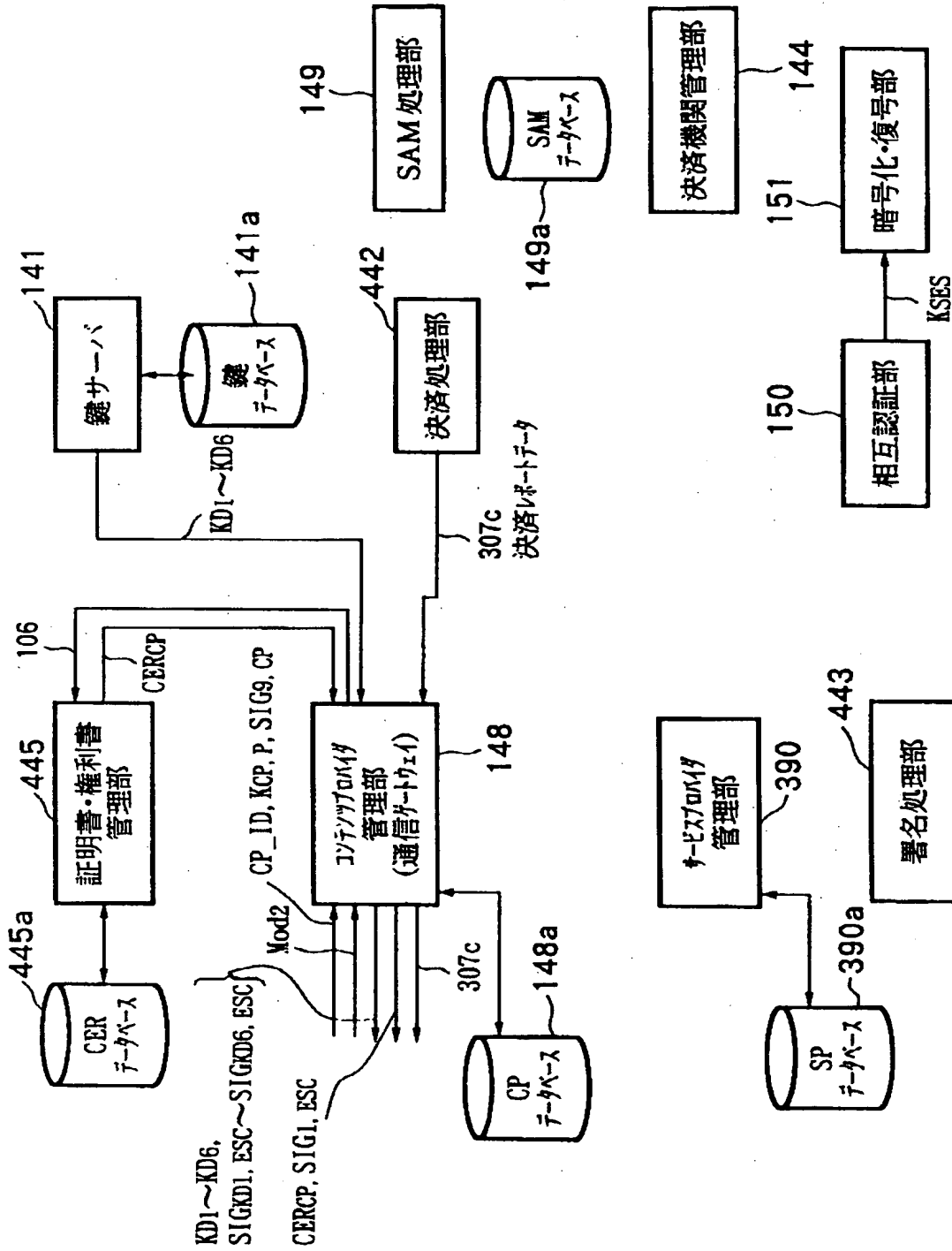


【图 5 6】

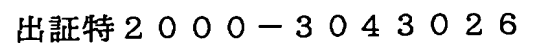


【図 57】

EMD サービスセンタ 302



EMD サービス センタ 302



【図 59】

利用履歴データ 308 の内容

識別子 Content_ID

識別子 CP_ID

識別子 SP_ID

コンテンツデータ C の信号諸元データ

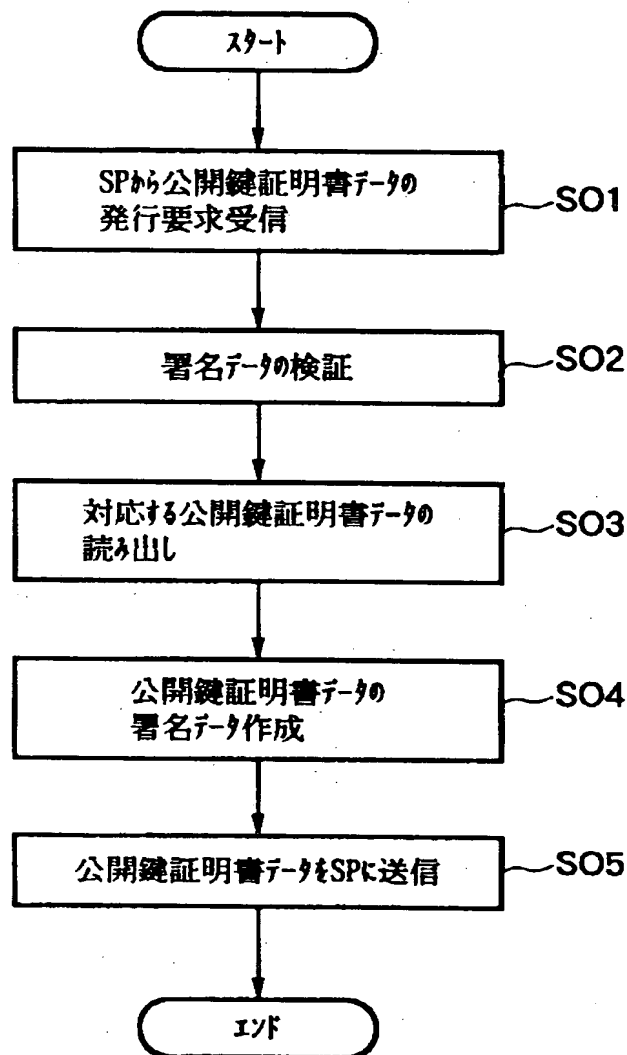
コンテンツデータ C の圧縮方法

記録媒体の識別子 Media_ID

識別子 SAM_ID、

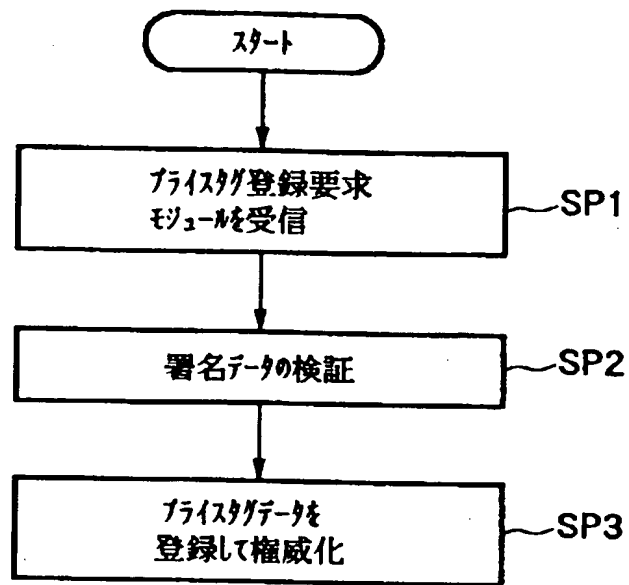
ユーザの USER_ID

【図 60】



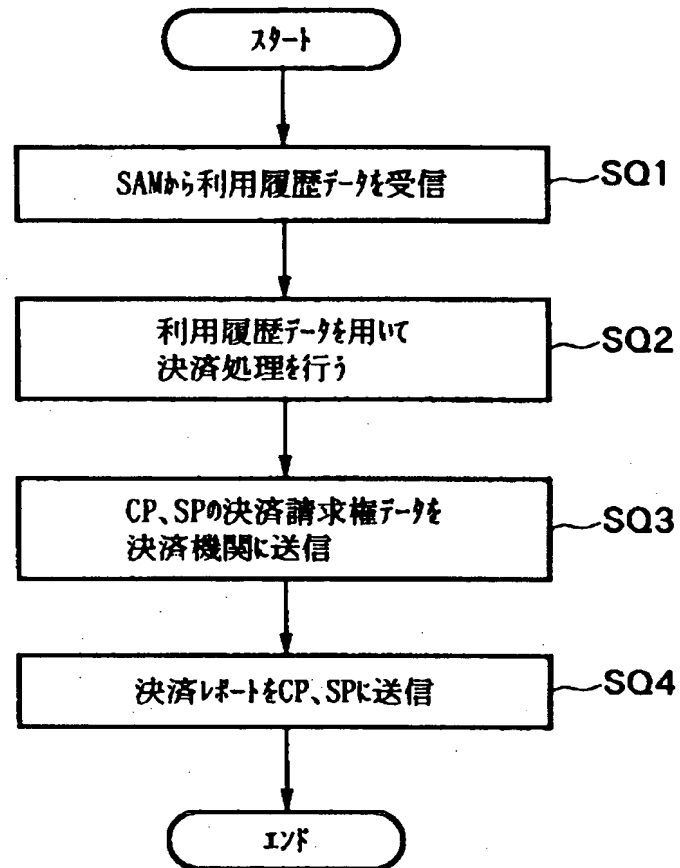
SPからの公開鍵証明書データの発行要求に応じたESCの処理

【図 61】



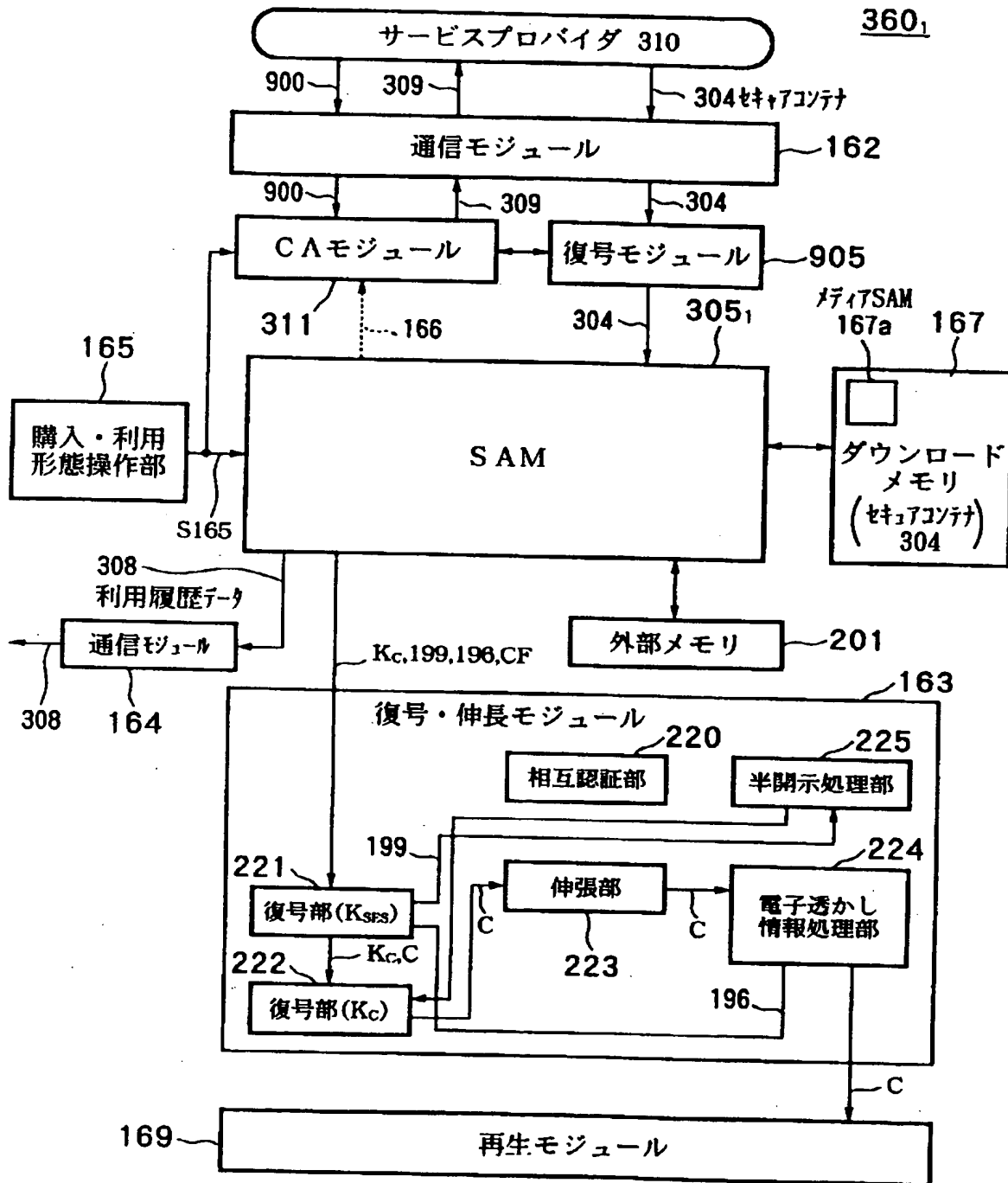
ESCにおけるライスタデータの登録処理

【図 62】

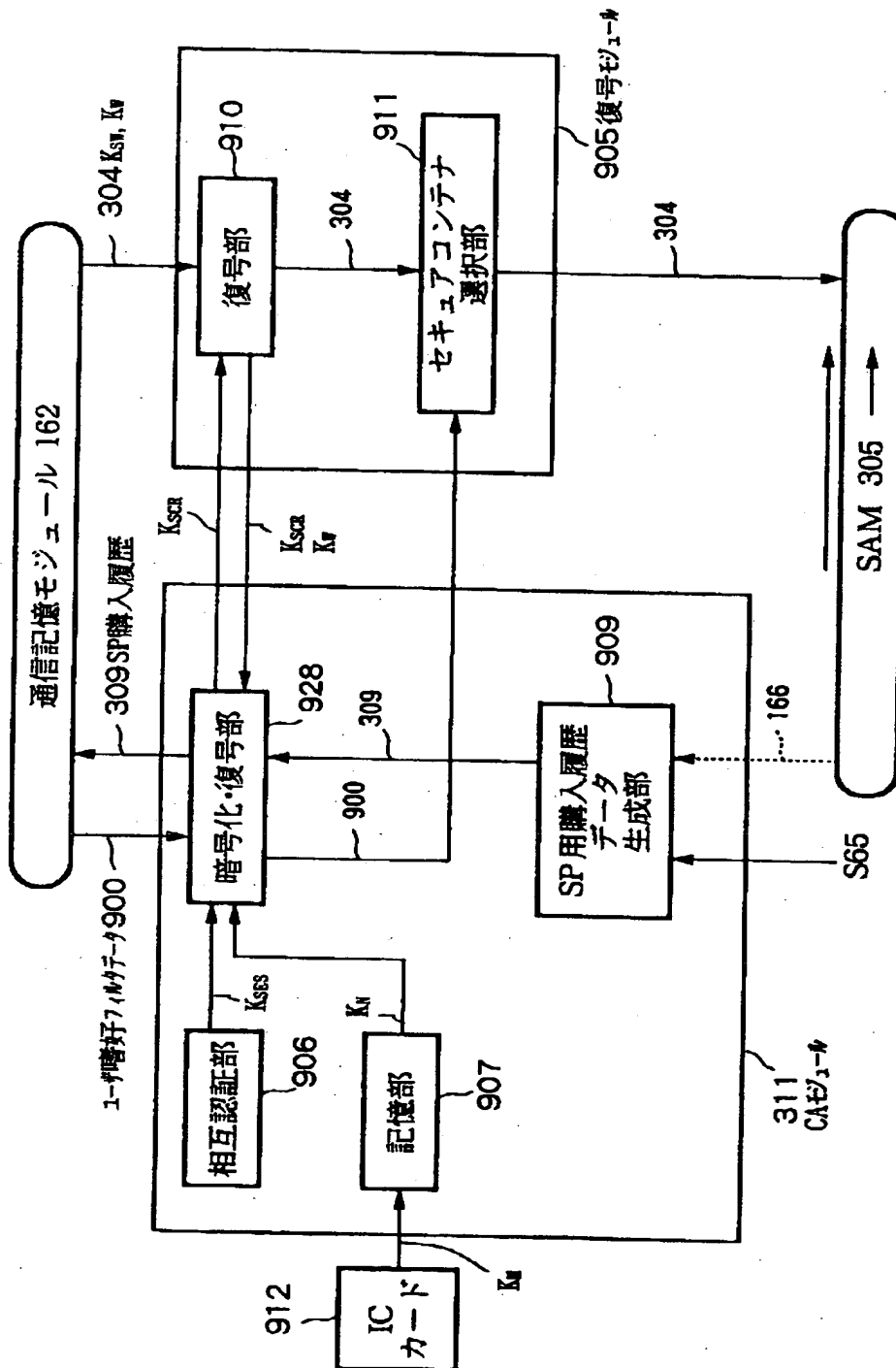


ESCによる決済処理

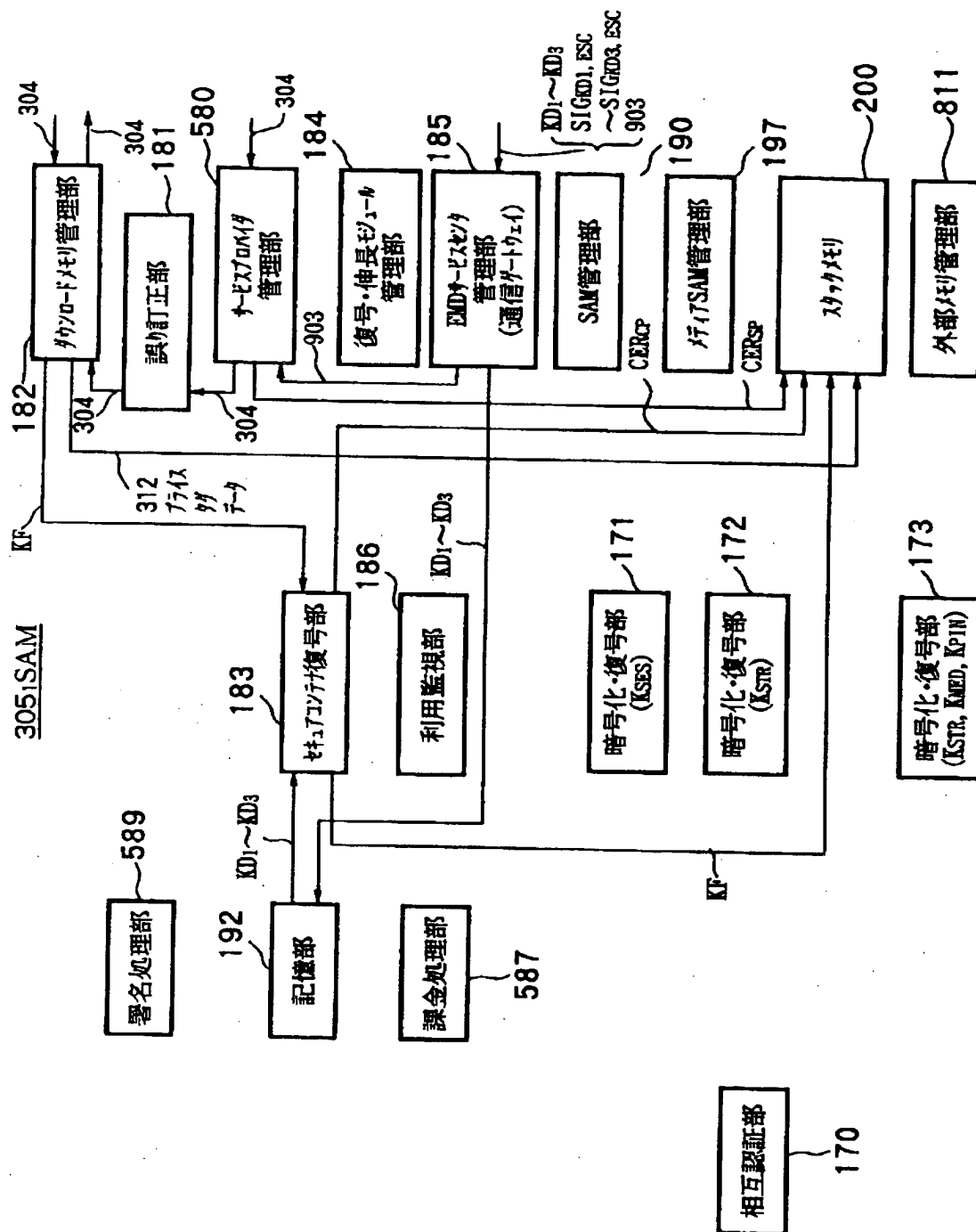
【図 63】



【图 6 4】



【図 6 5】



【図66】

スタックメモリ200の記憶データ

コンテンツ鍵データ K_c

権利書データ (UCP) 106

不揮発性メモリ201のロック鍵データ K_{Loc}

コンテンツプロバイダ301の公開鍵証明書データ CER_{cp}

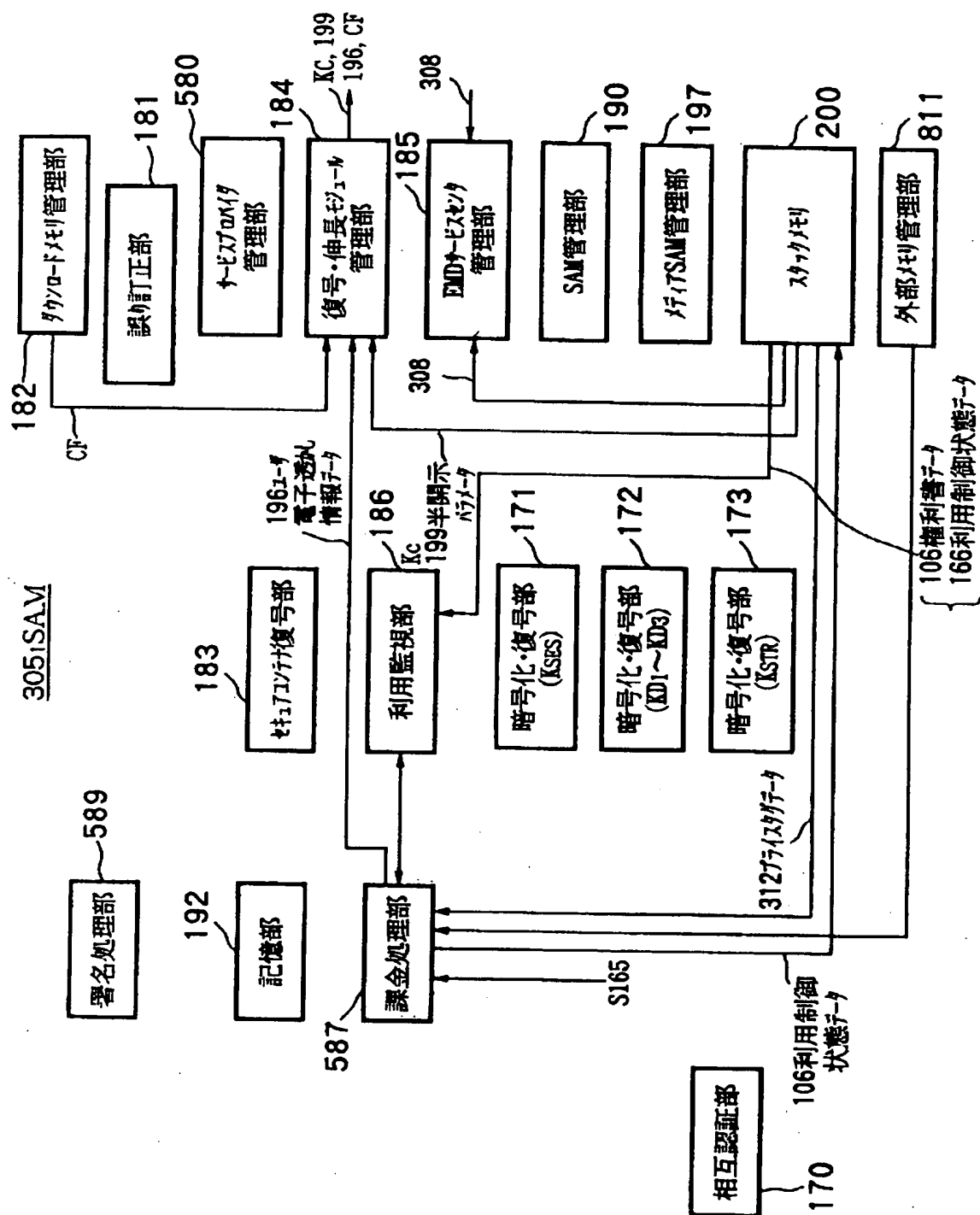
サービスプロバイダ301の公開鍵証明書データ CER_{sp}

利用制御情状態データ (UCS) 166

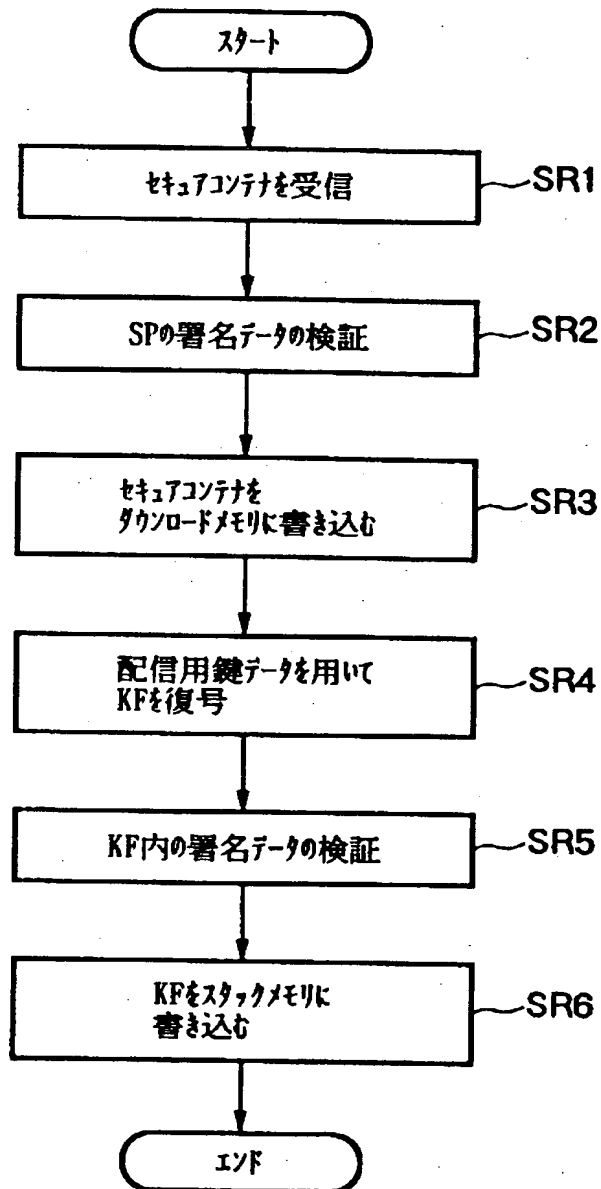
SAMプログラム・ダウンロード・コンテナ $SD_1 \sim SDC_3$

プライスタグデータ 312

【图 6 7】

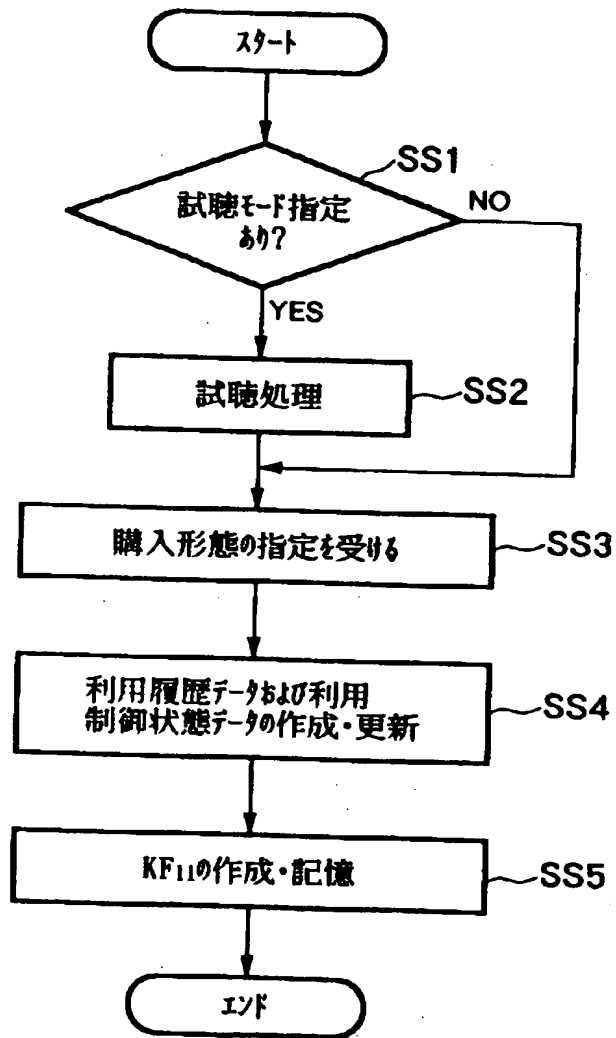


【図 68】



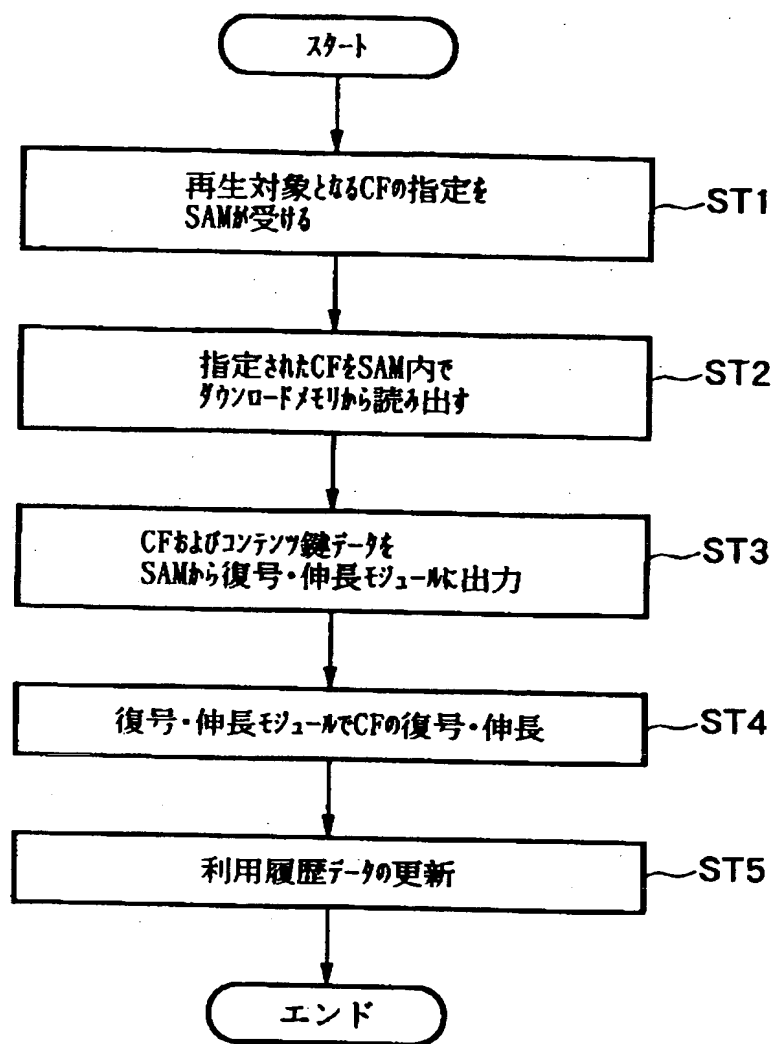
SAMにおけるKFの復号処理

【図 69】



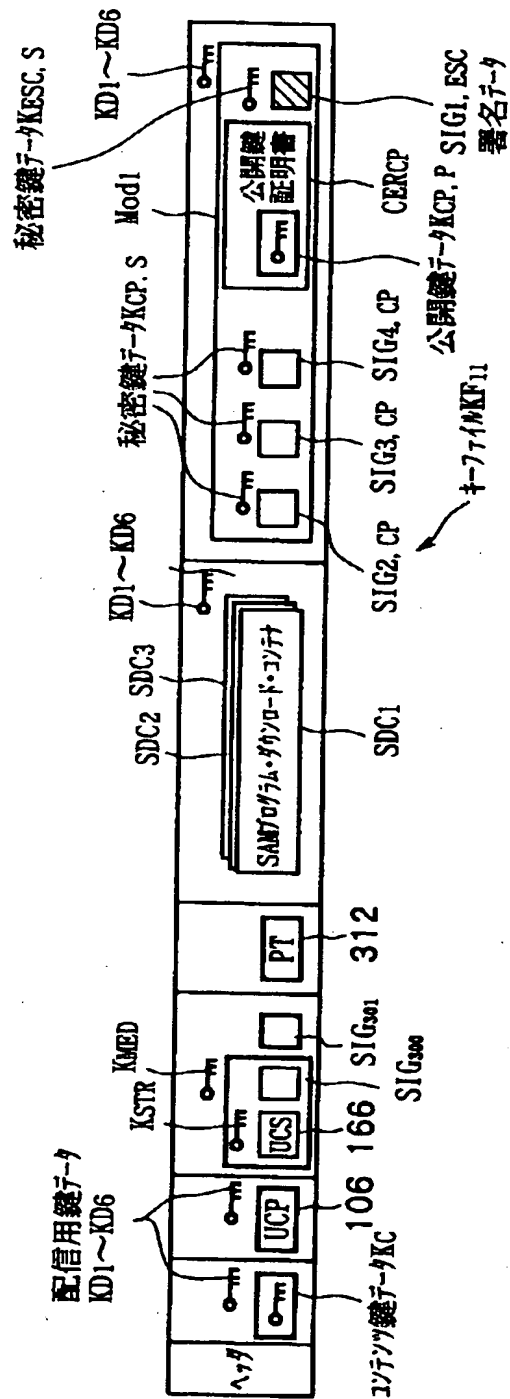
SAMにおけるセキュアコンテンツの購入形態決定処理

【図 70】

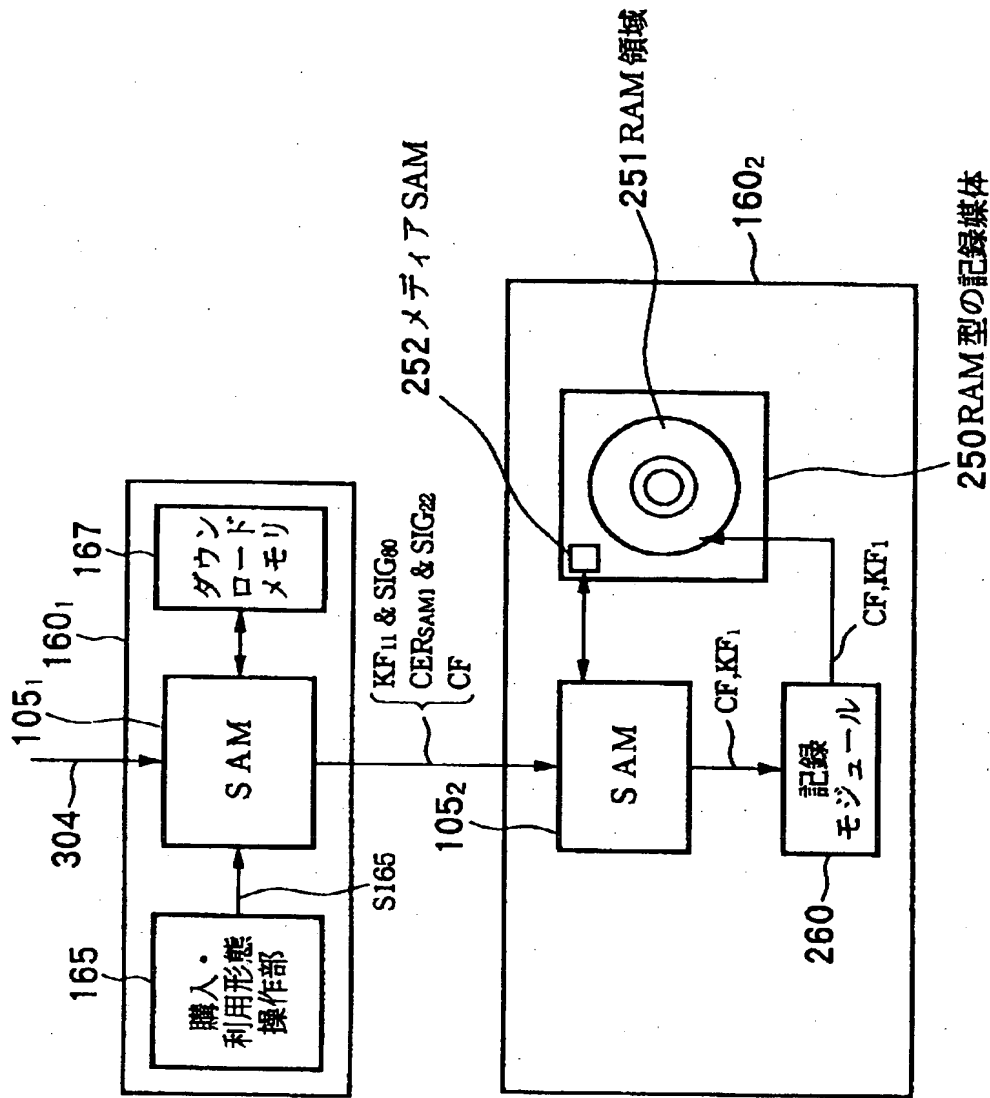


コンテンツデータの再生処理

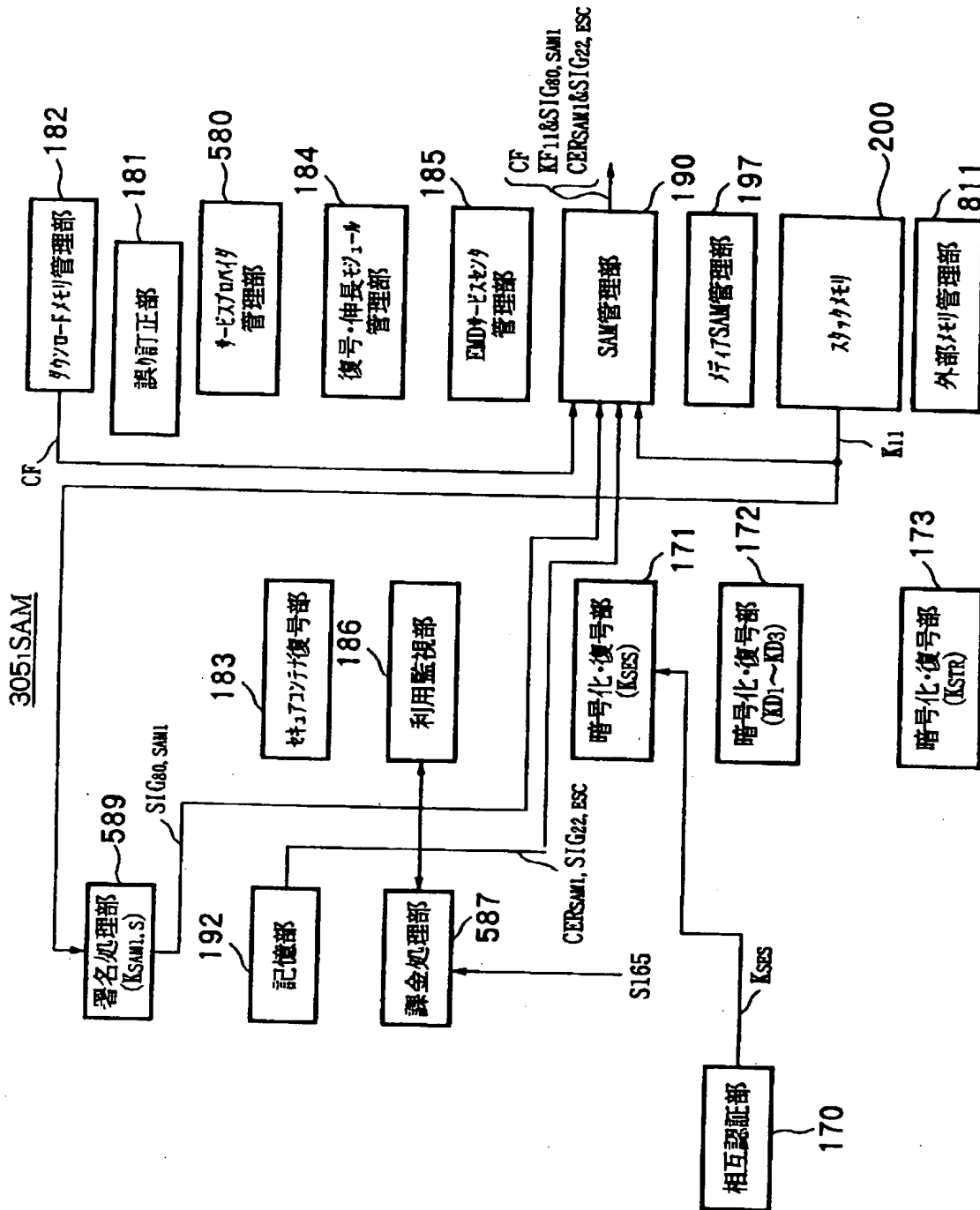
【圖 7 1】



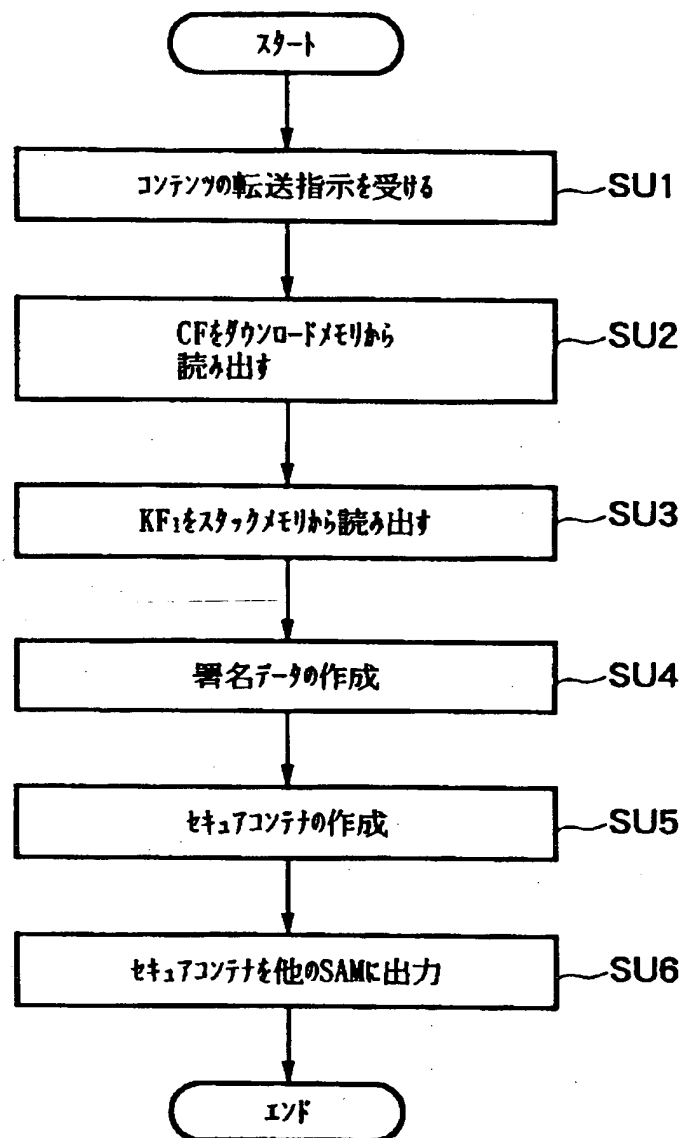
【図 7 2】



【図 73】

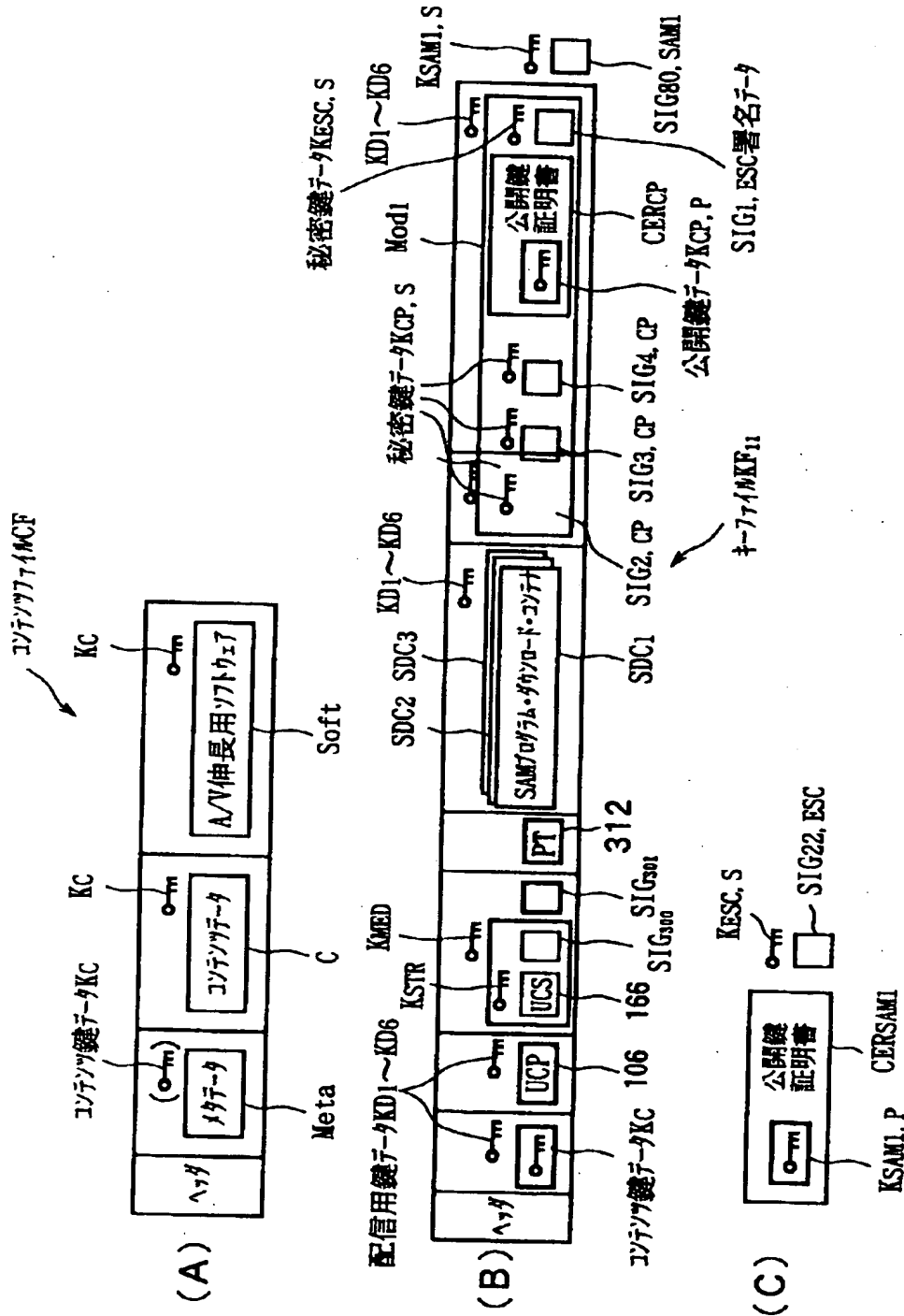


【図 7 4】

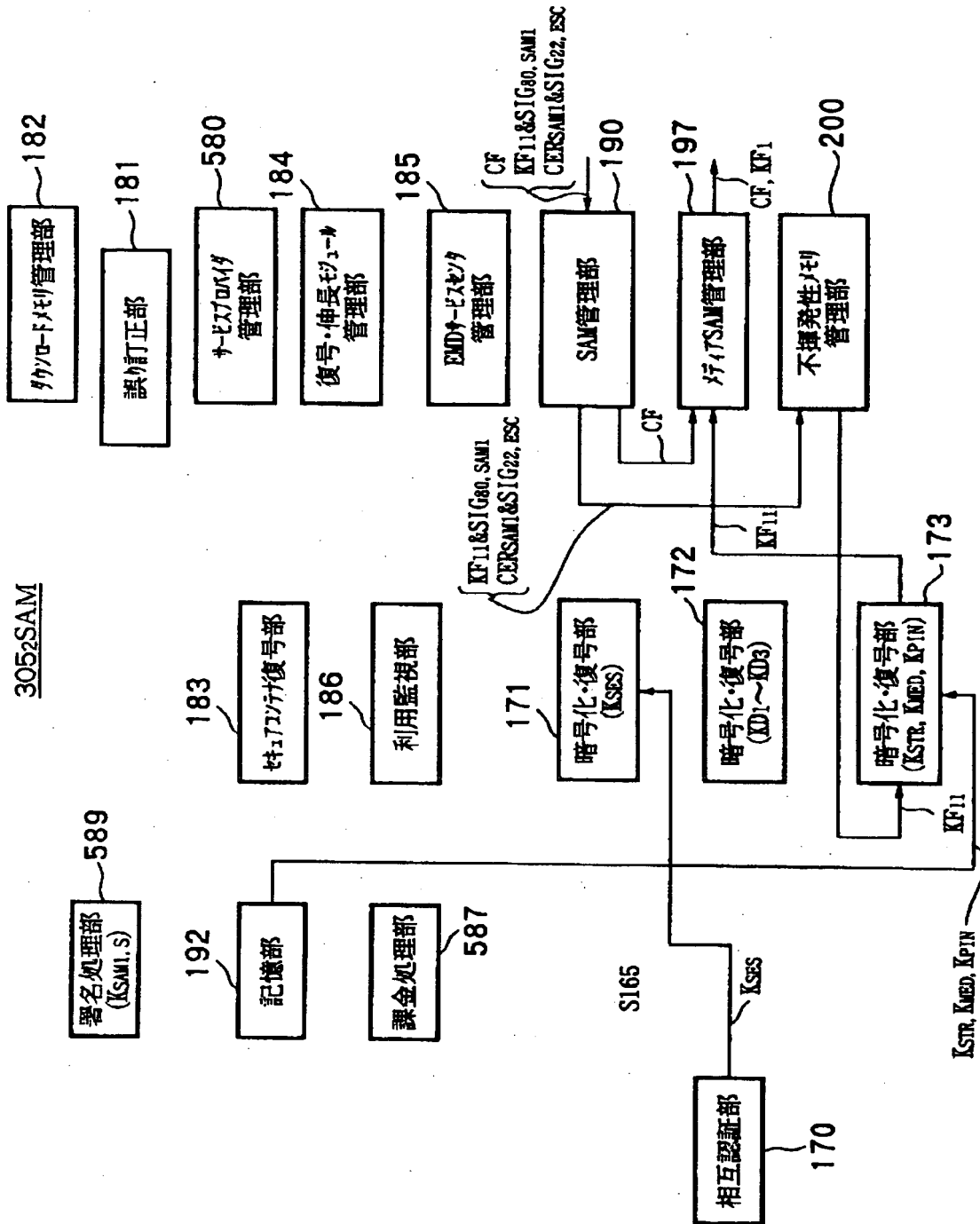


購入形態決定後のコンテンツを他のSAMに転送するSAMの処理

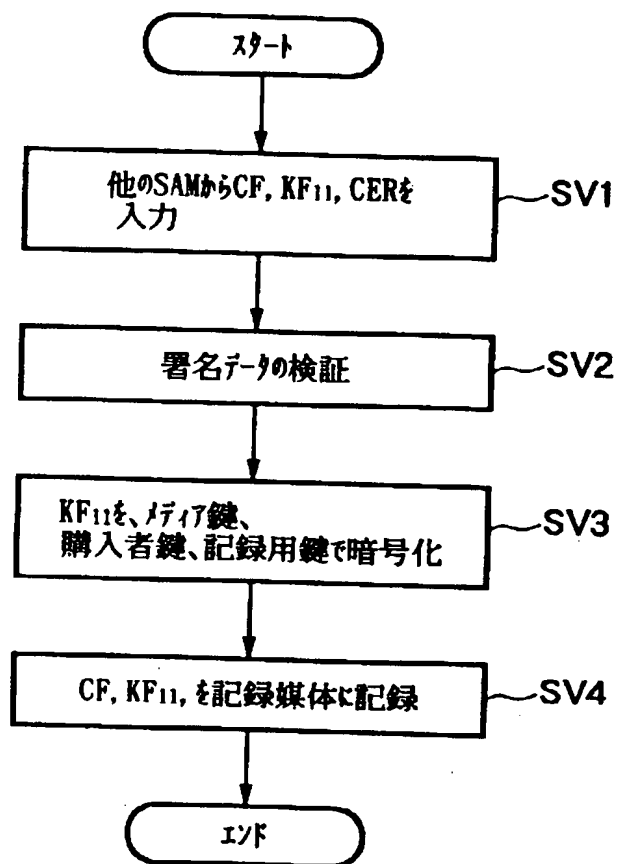
【図 75】



【図 76】

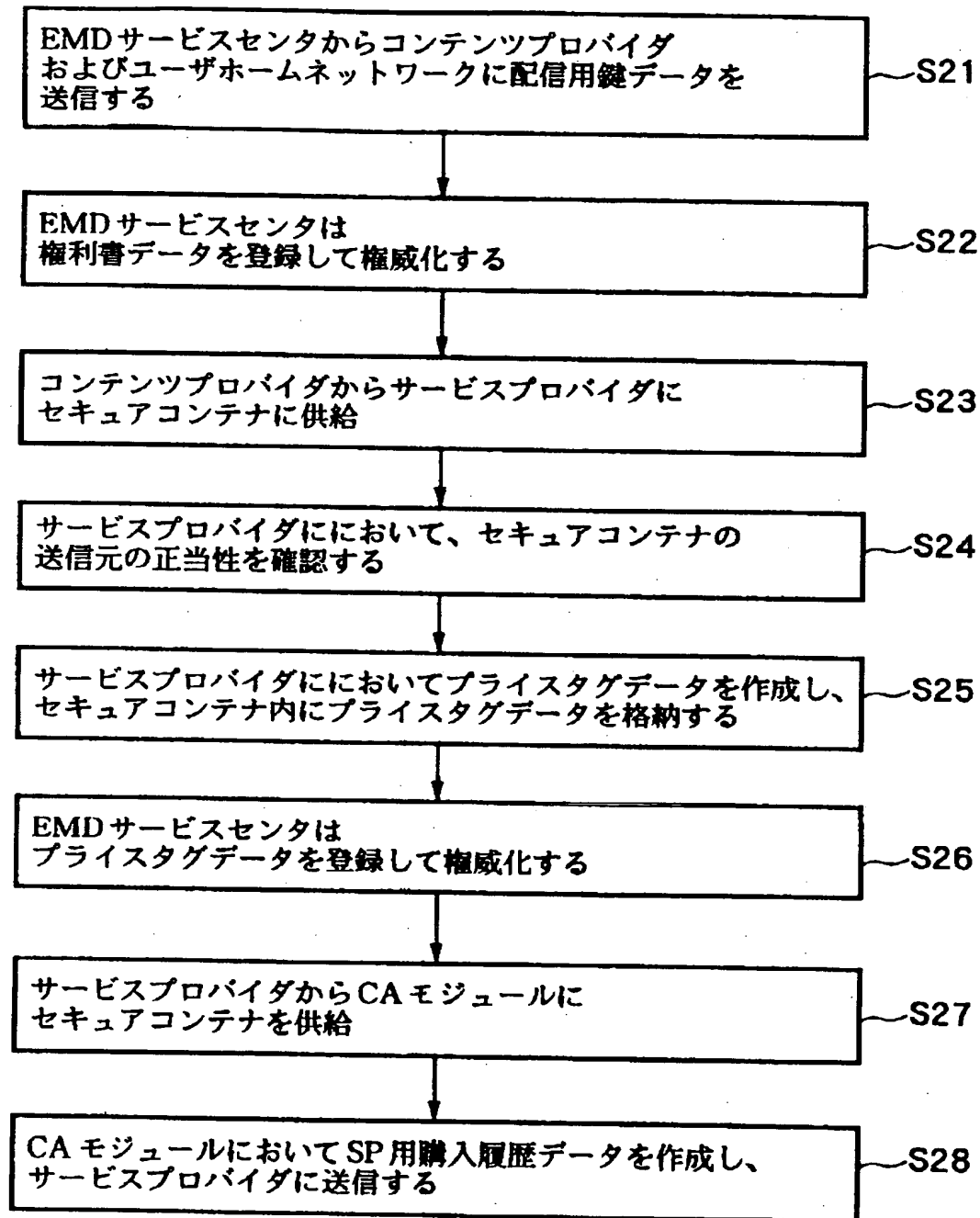


【図 77】

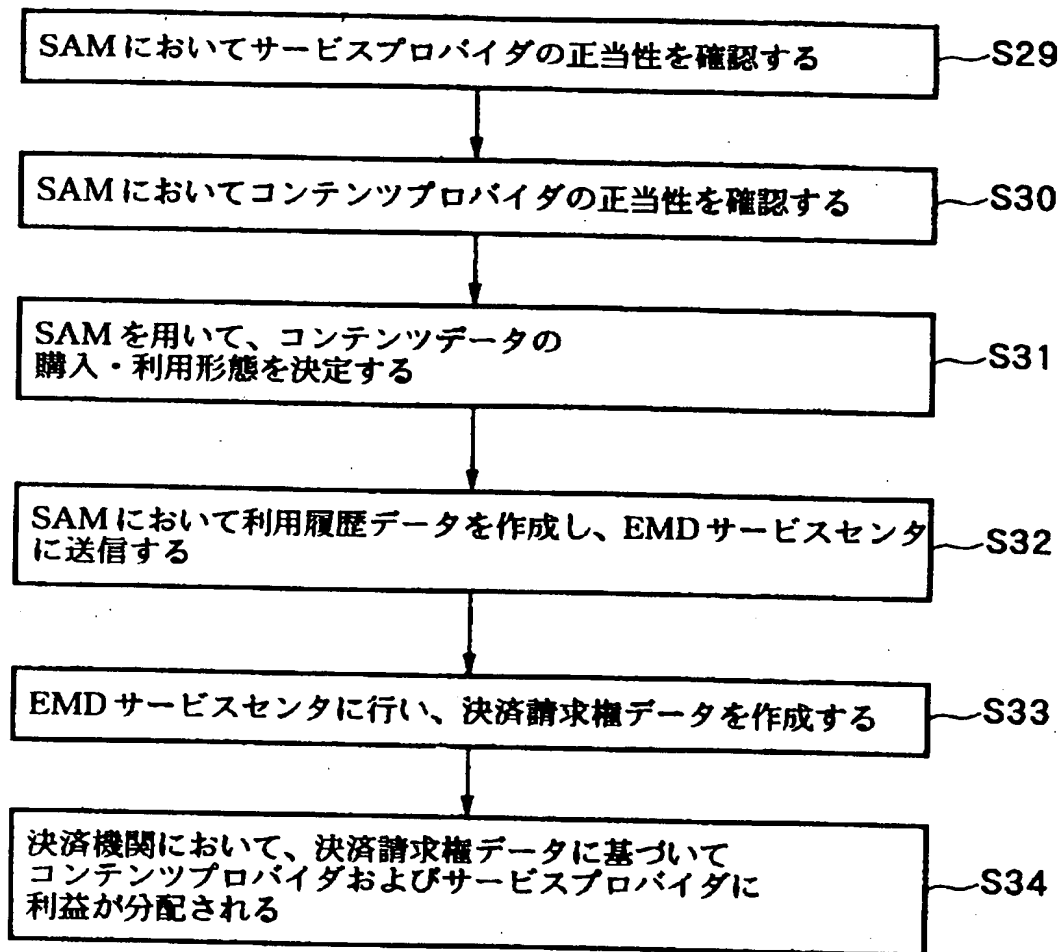


他のSAMから入力したCF等を記録媒体に書き込む際のSAMの処理

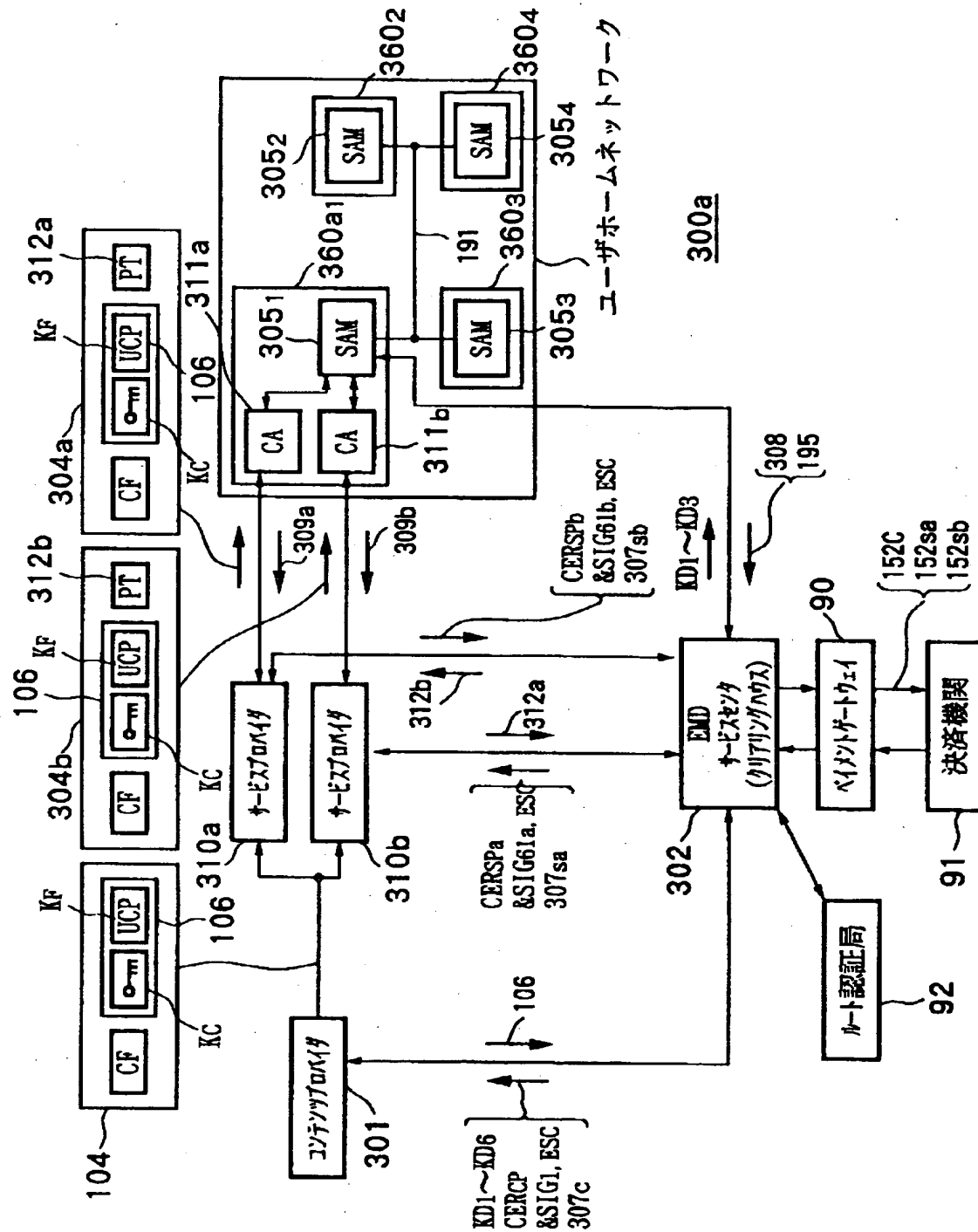
【図 78】



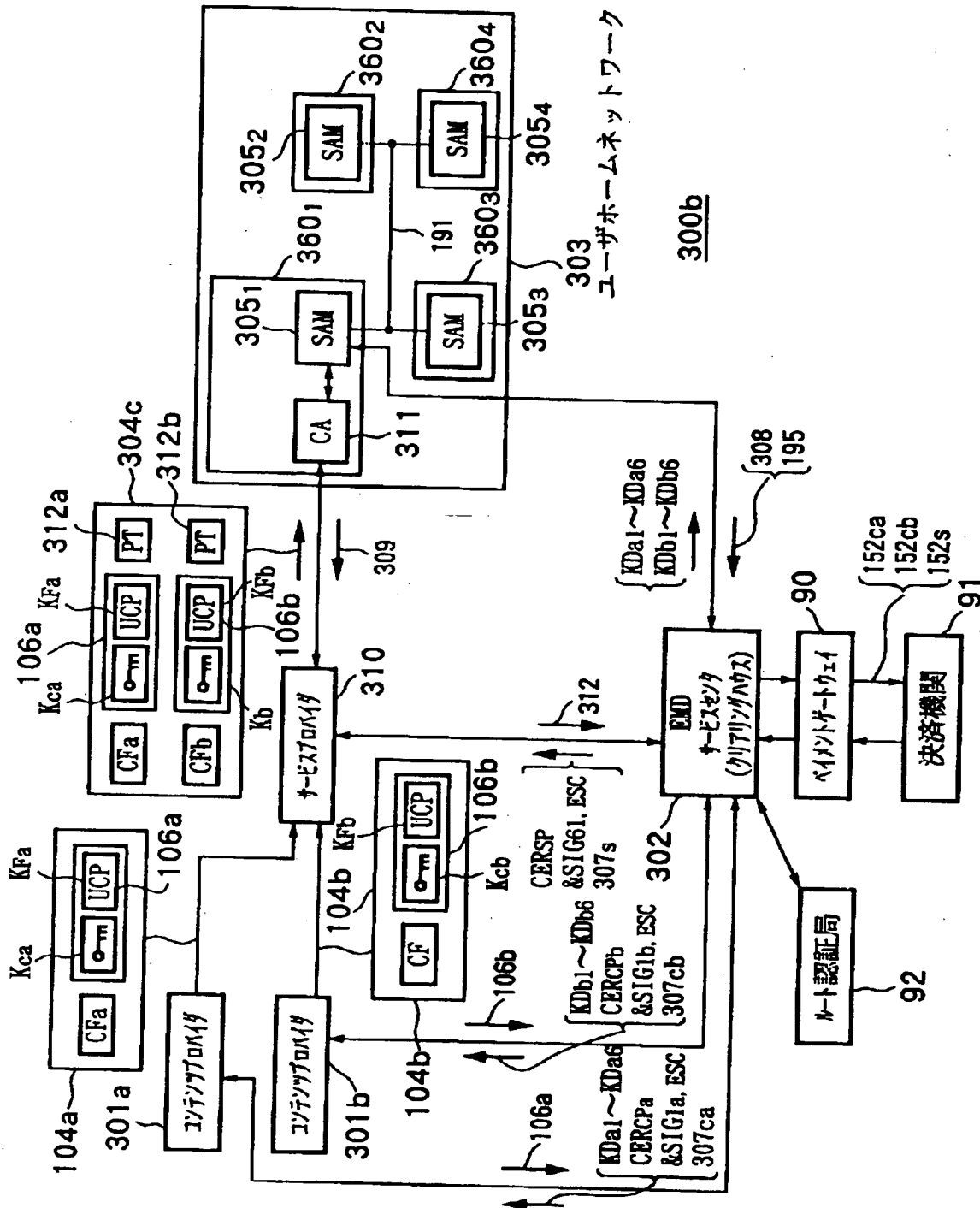
【図 79】



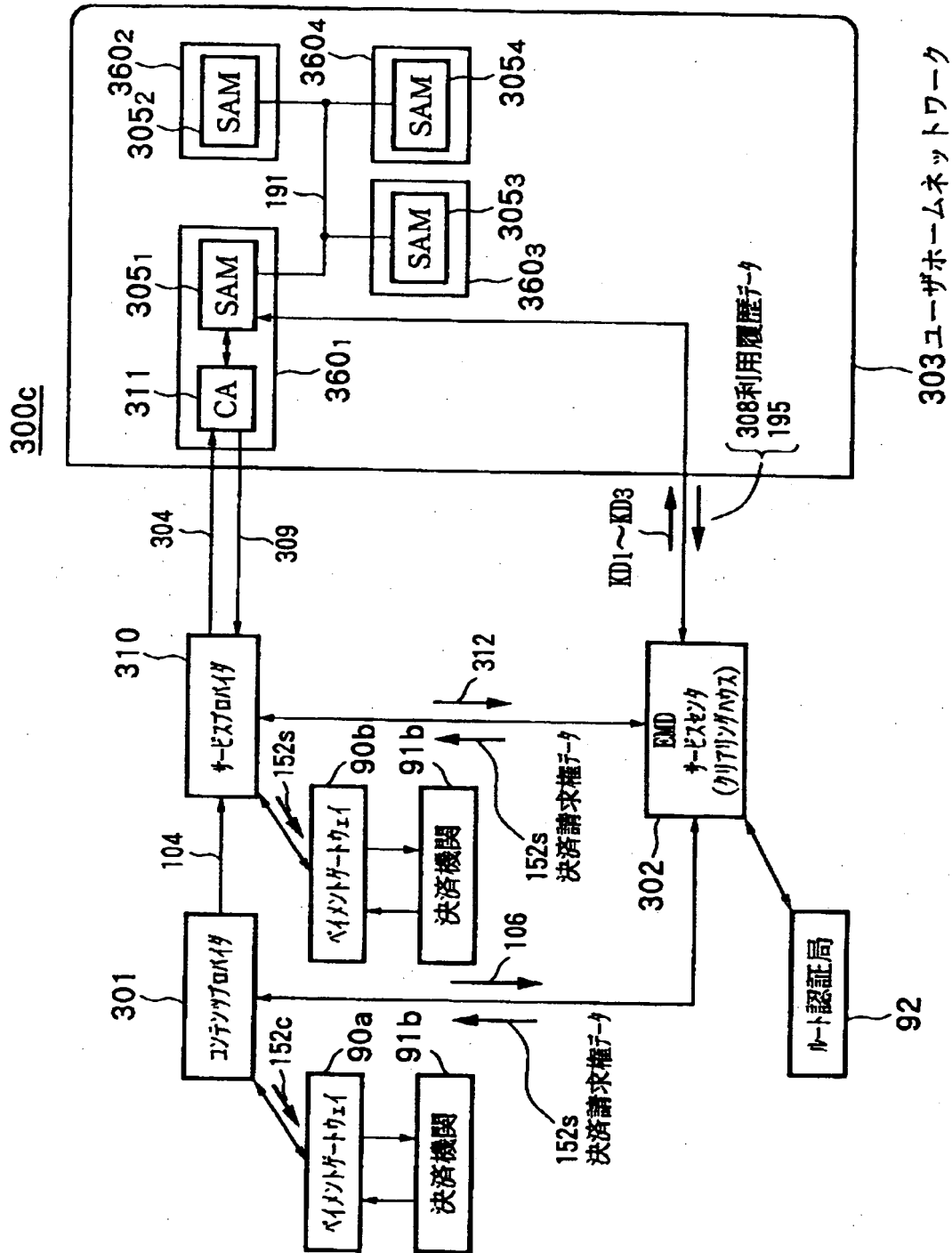
【図 80】



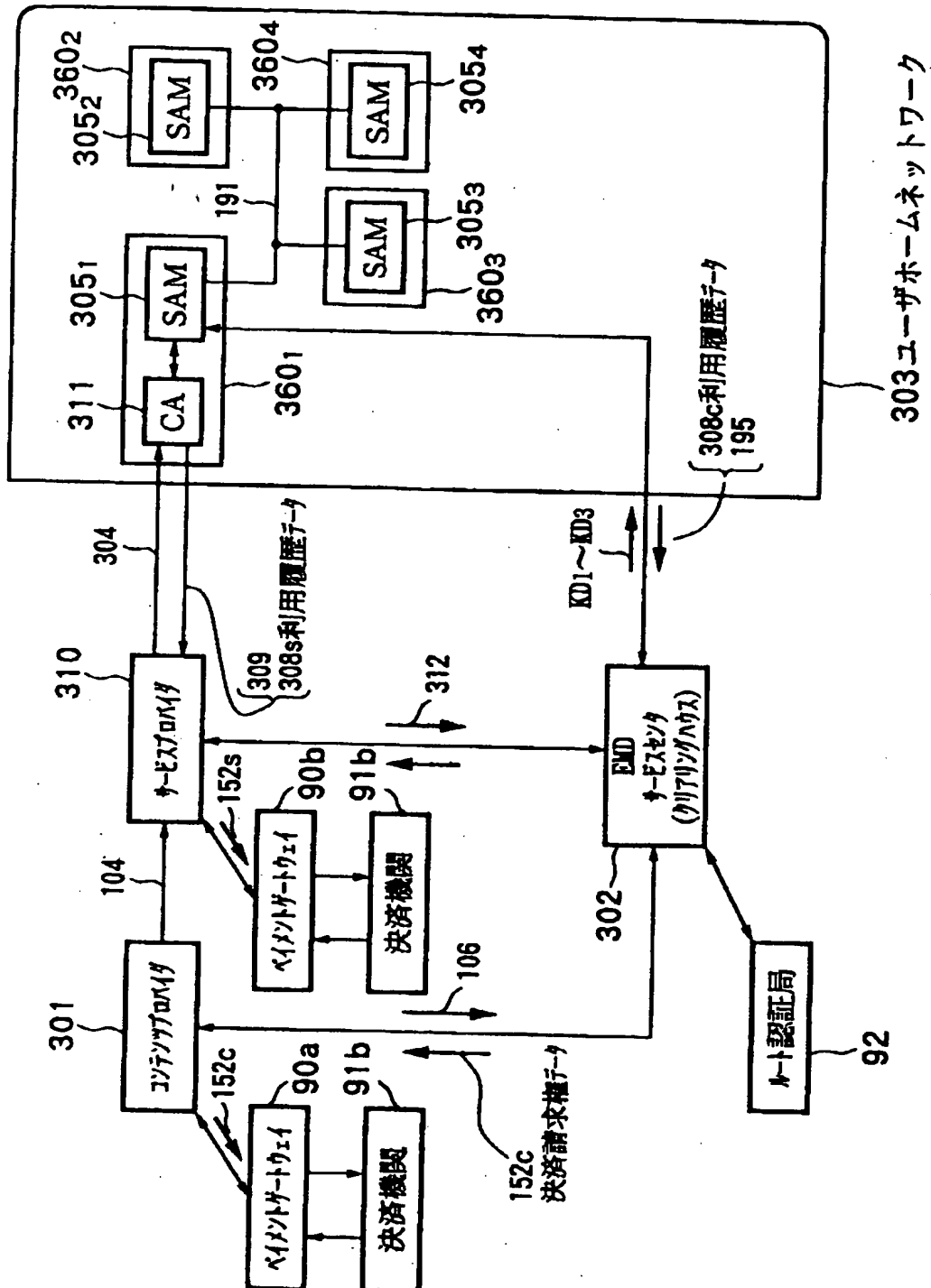
【図 81】



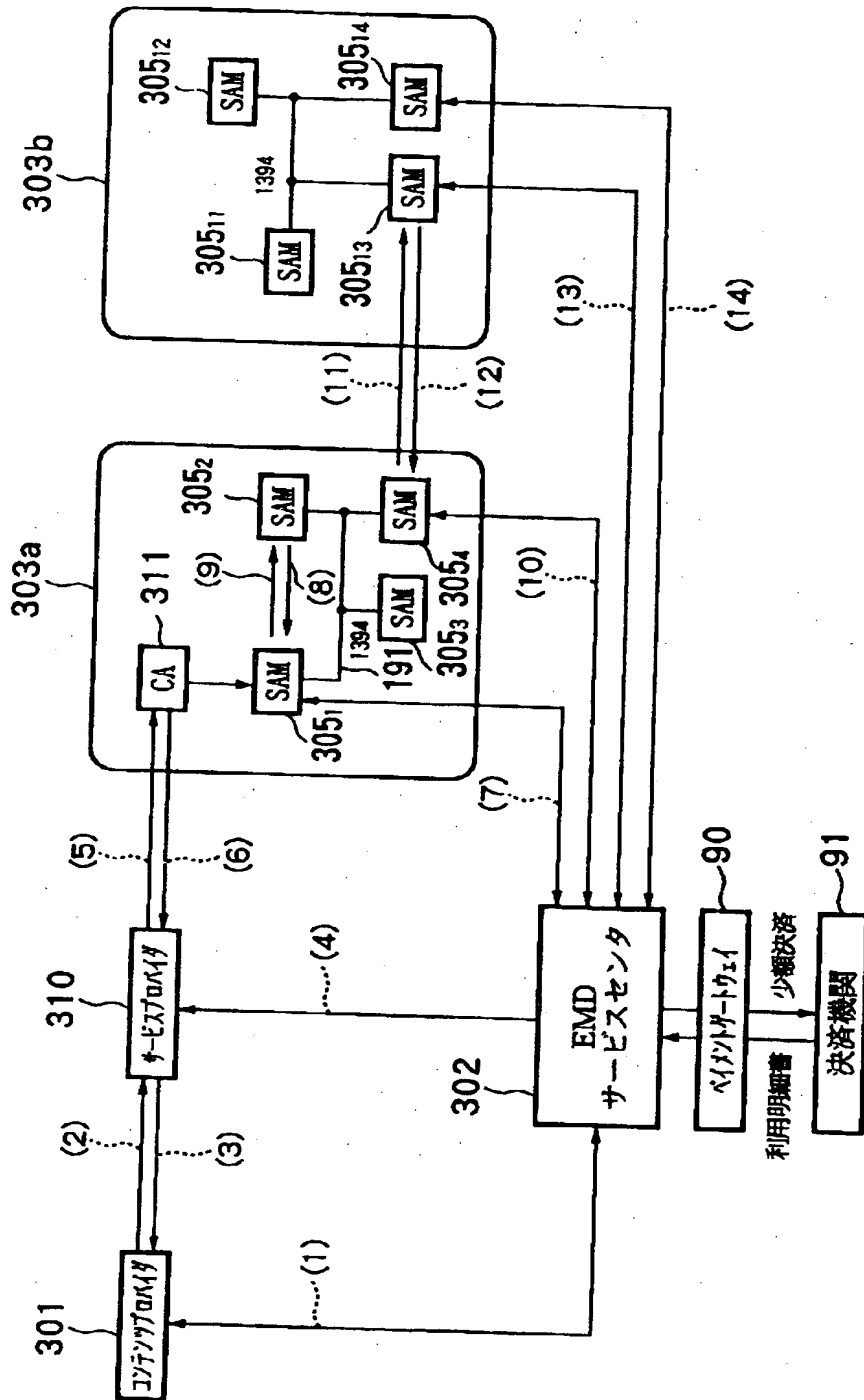
【図 82】



【图 8 3】

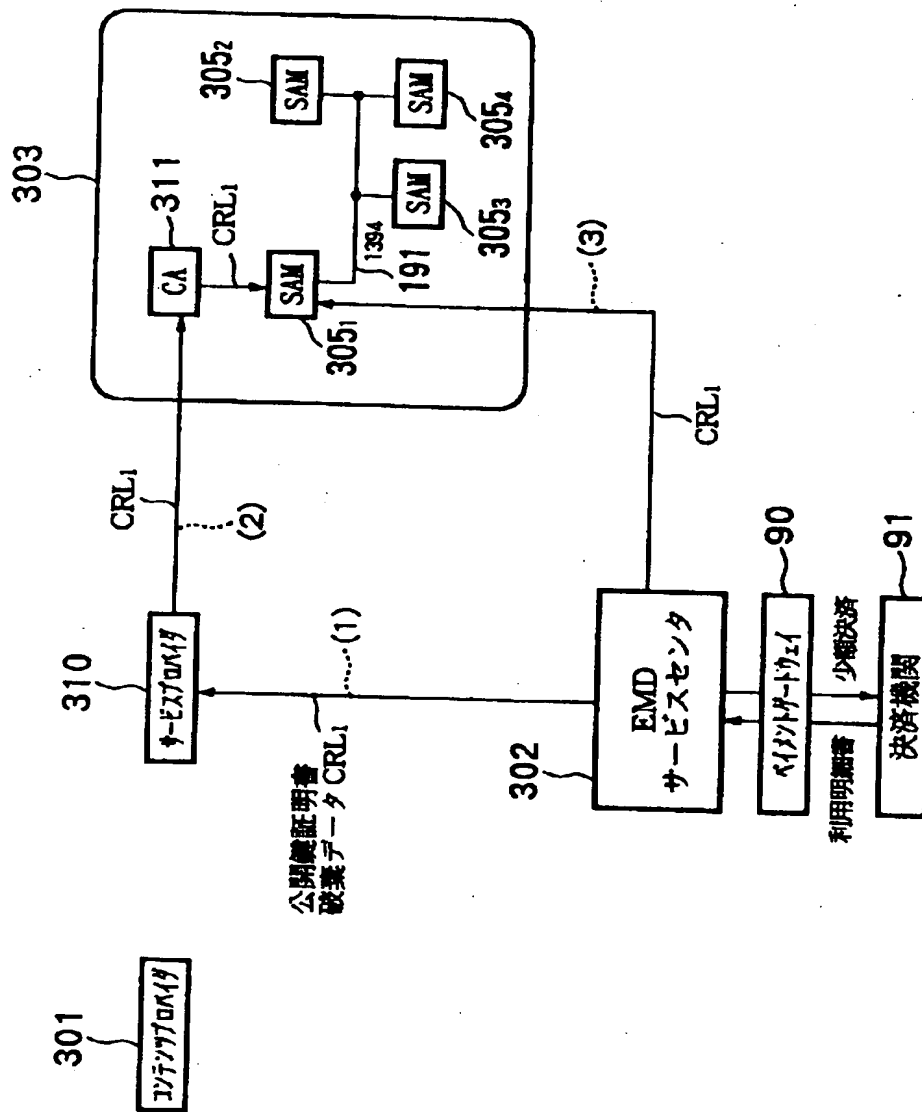


【図 84】



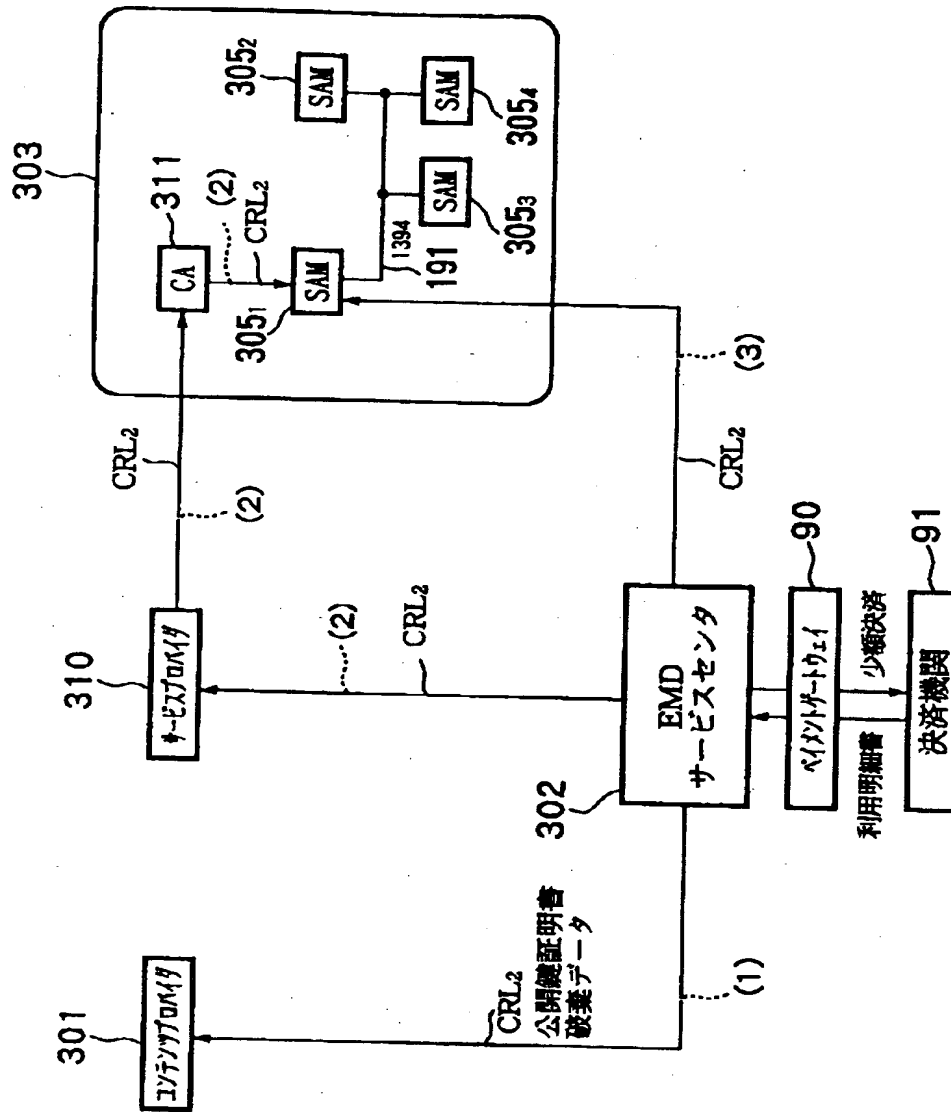
公開鍵証明書の手ルート

【図 8 5】



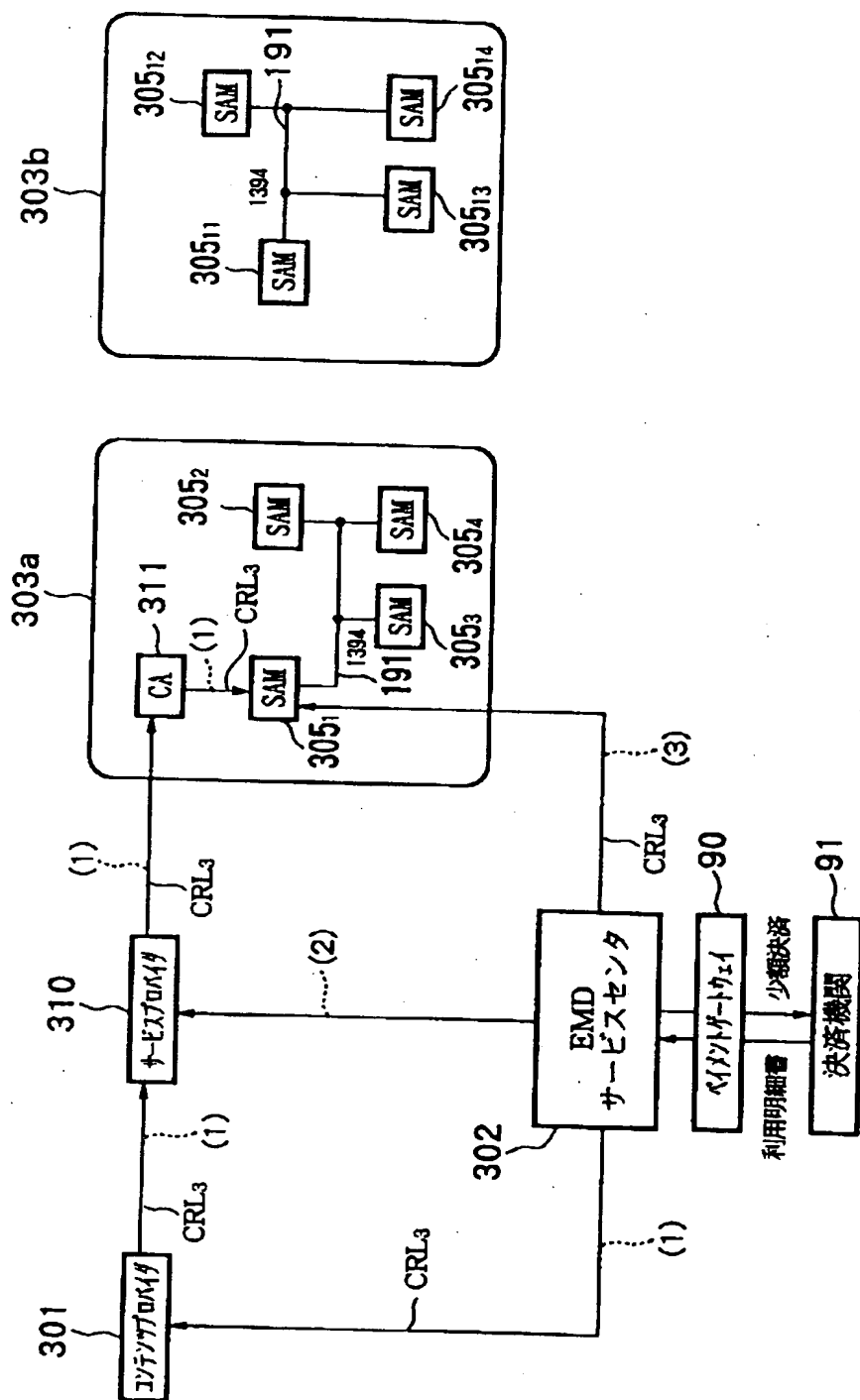
CERCPを無効にする場合

【図 86】



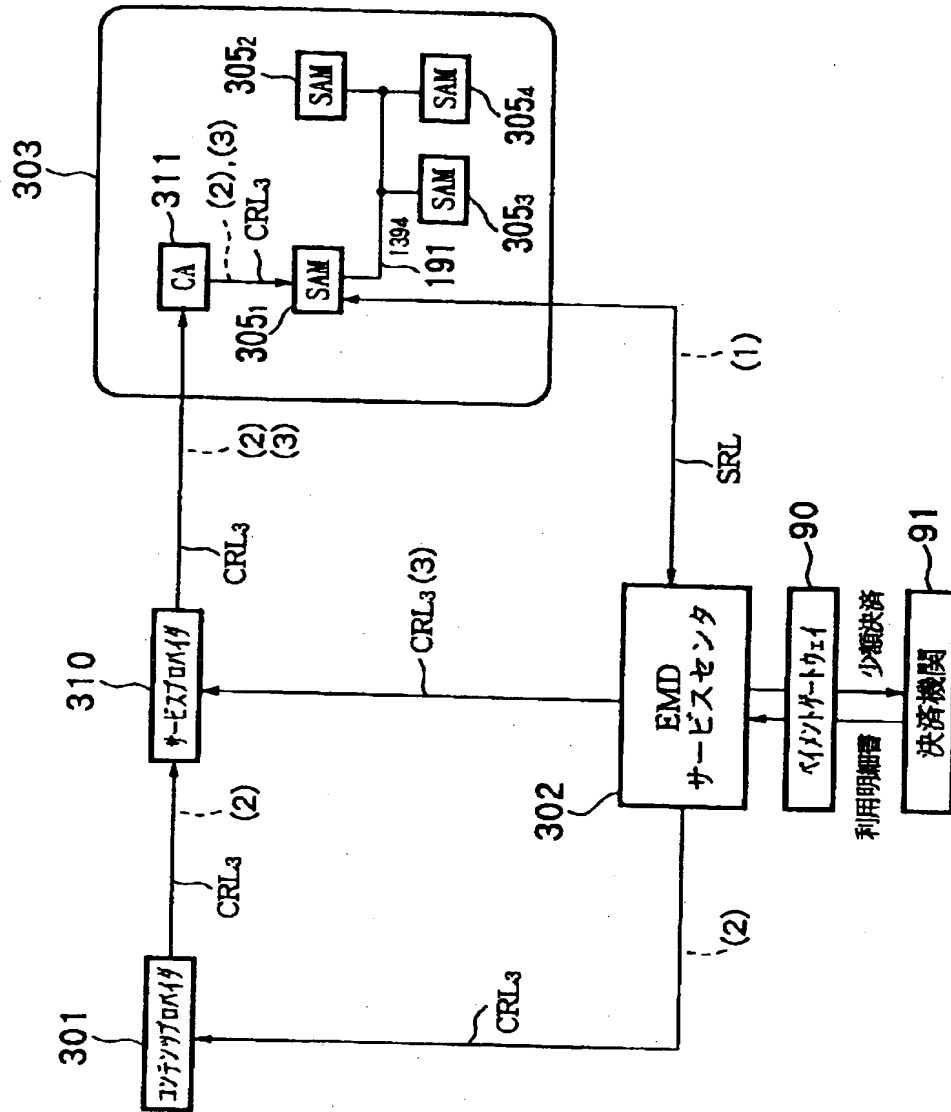
CERSPを無効にする場合

【図 87】

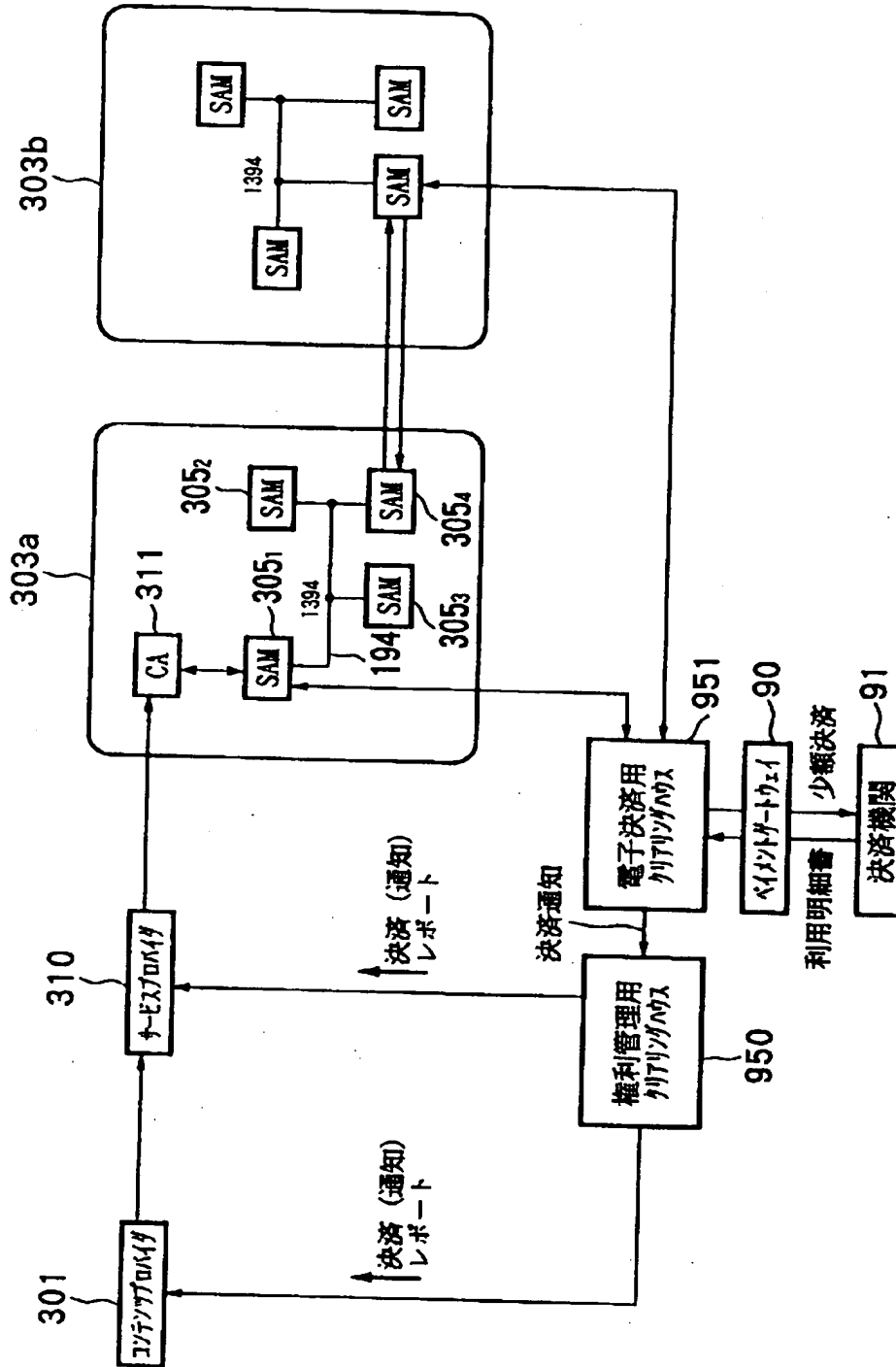


CERSAM2 を無効にする場合

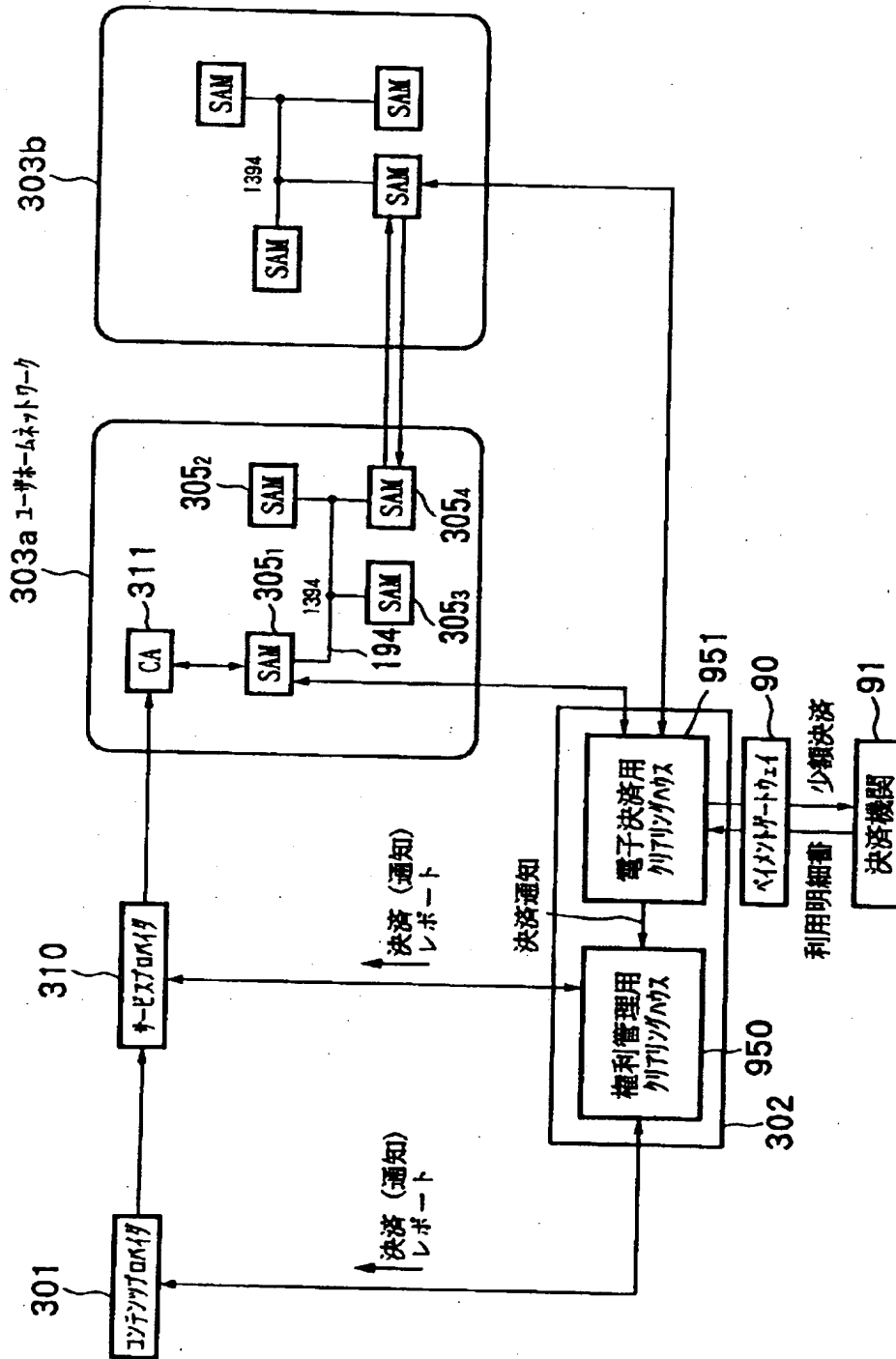
【図88】



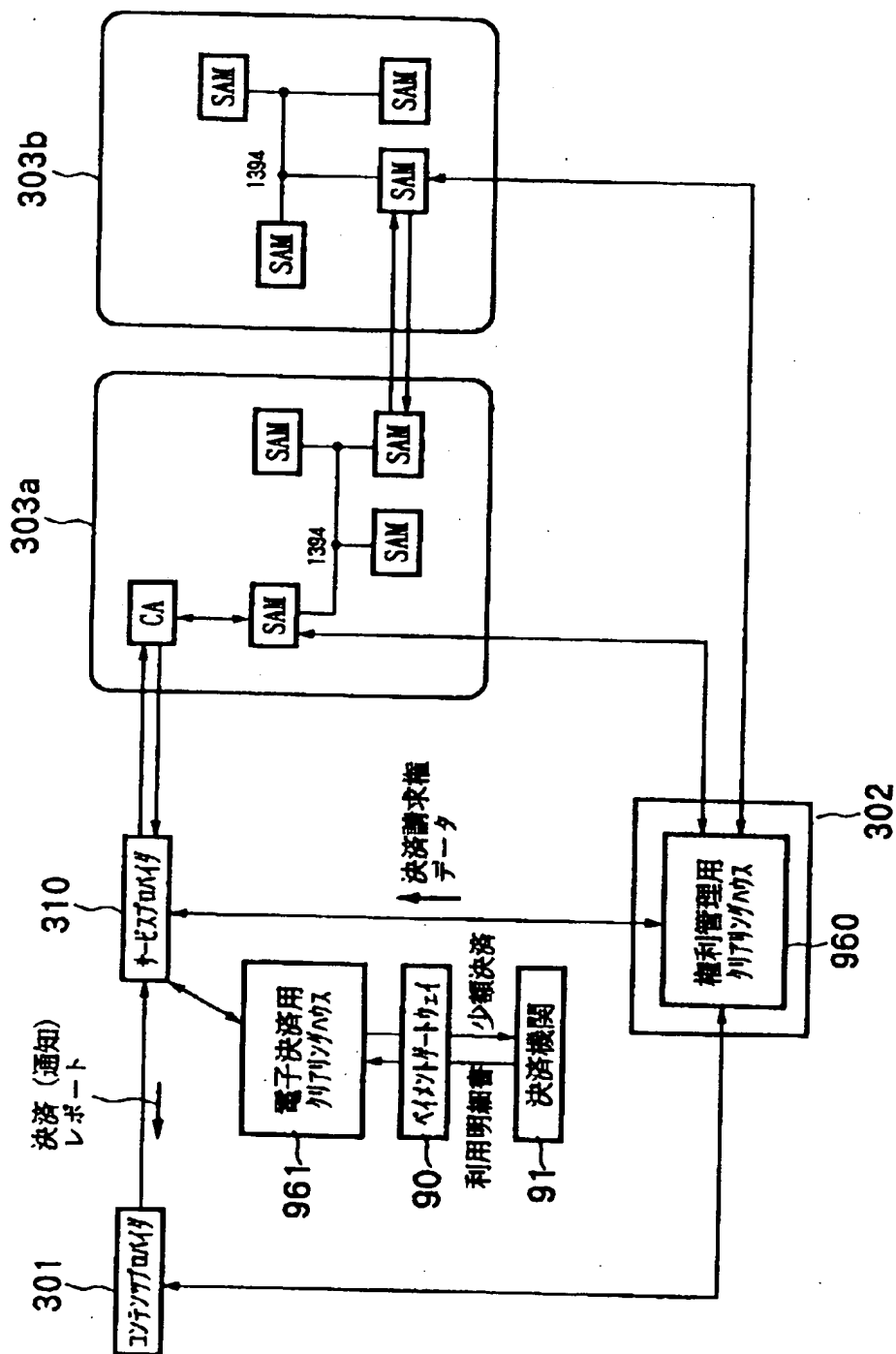
【図 89】



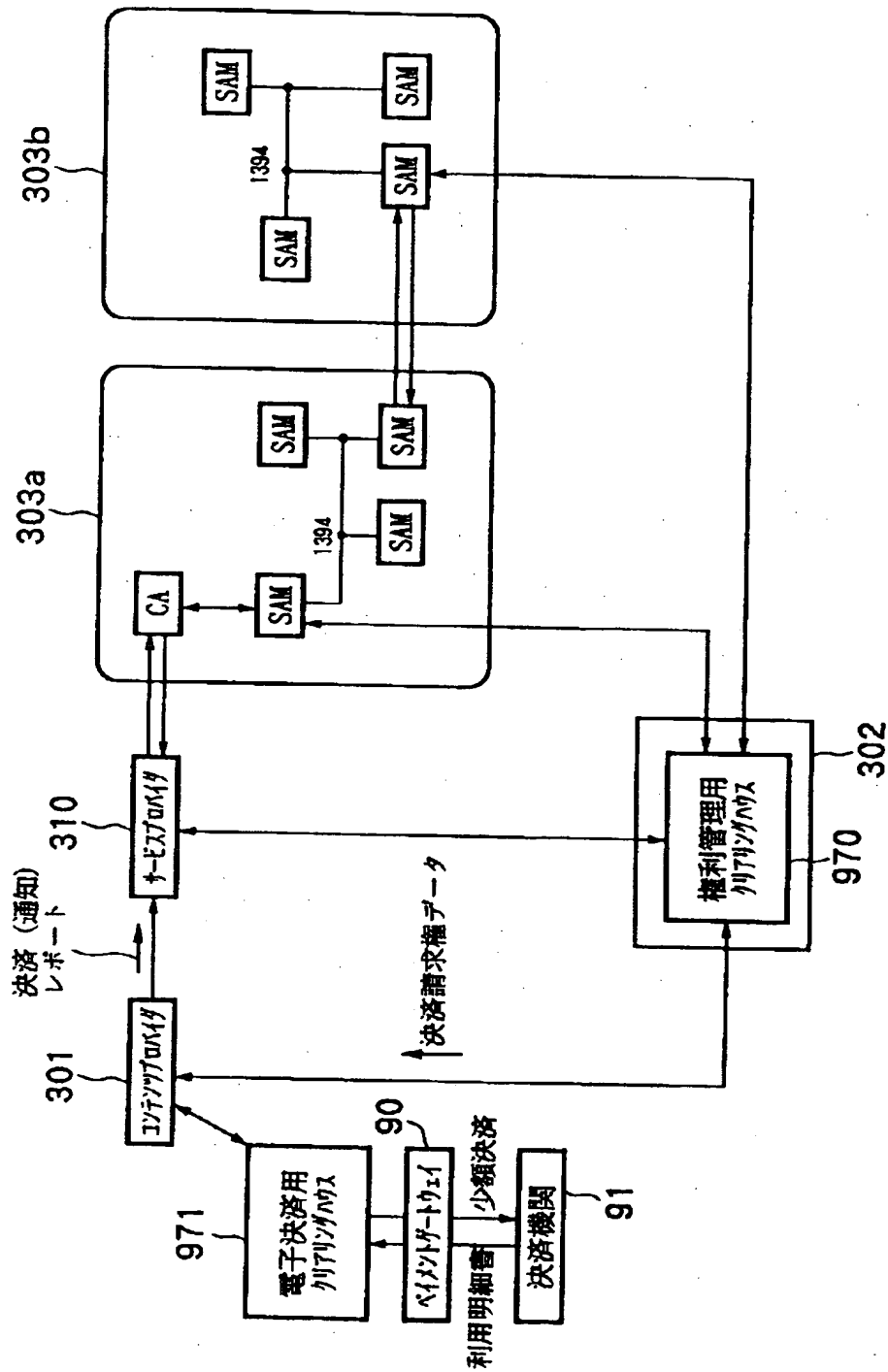
【図 90】



【図 91】

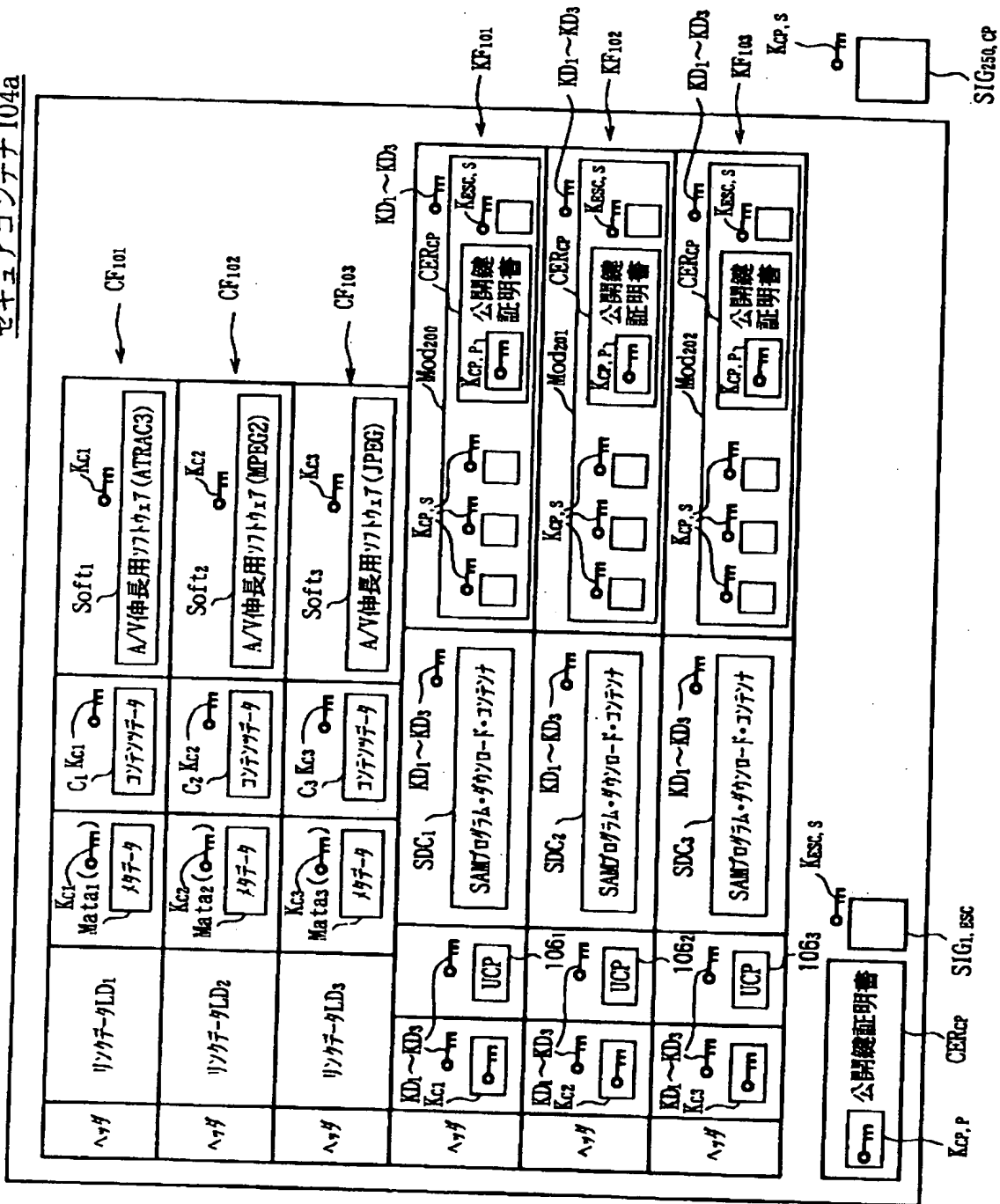


【図 9 2】

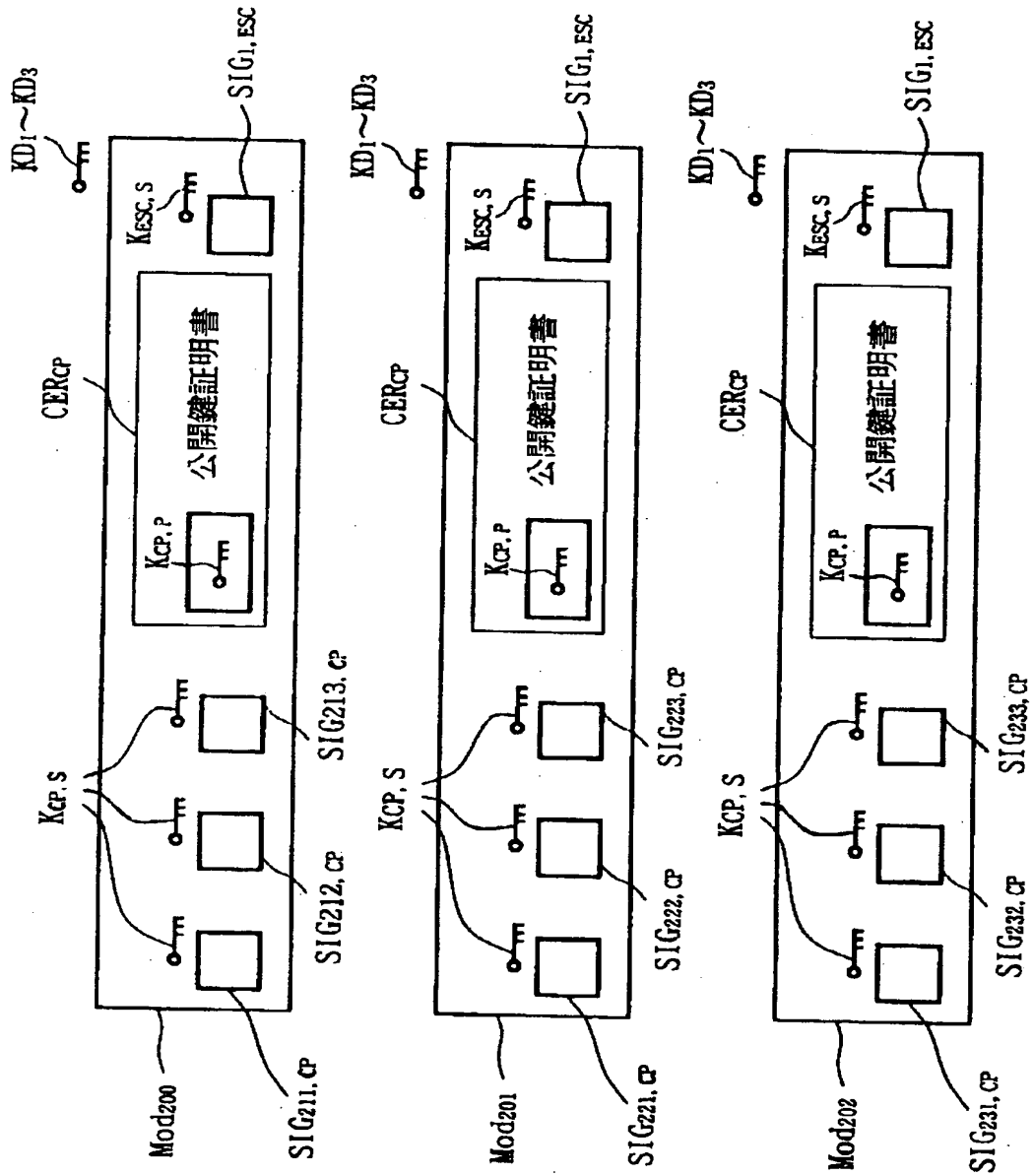


【図 93】

セキュアコンテナ104a

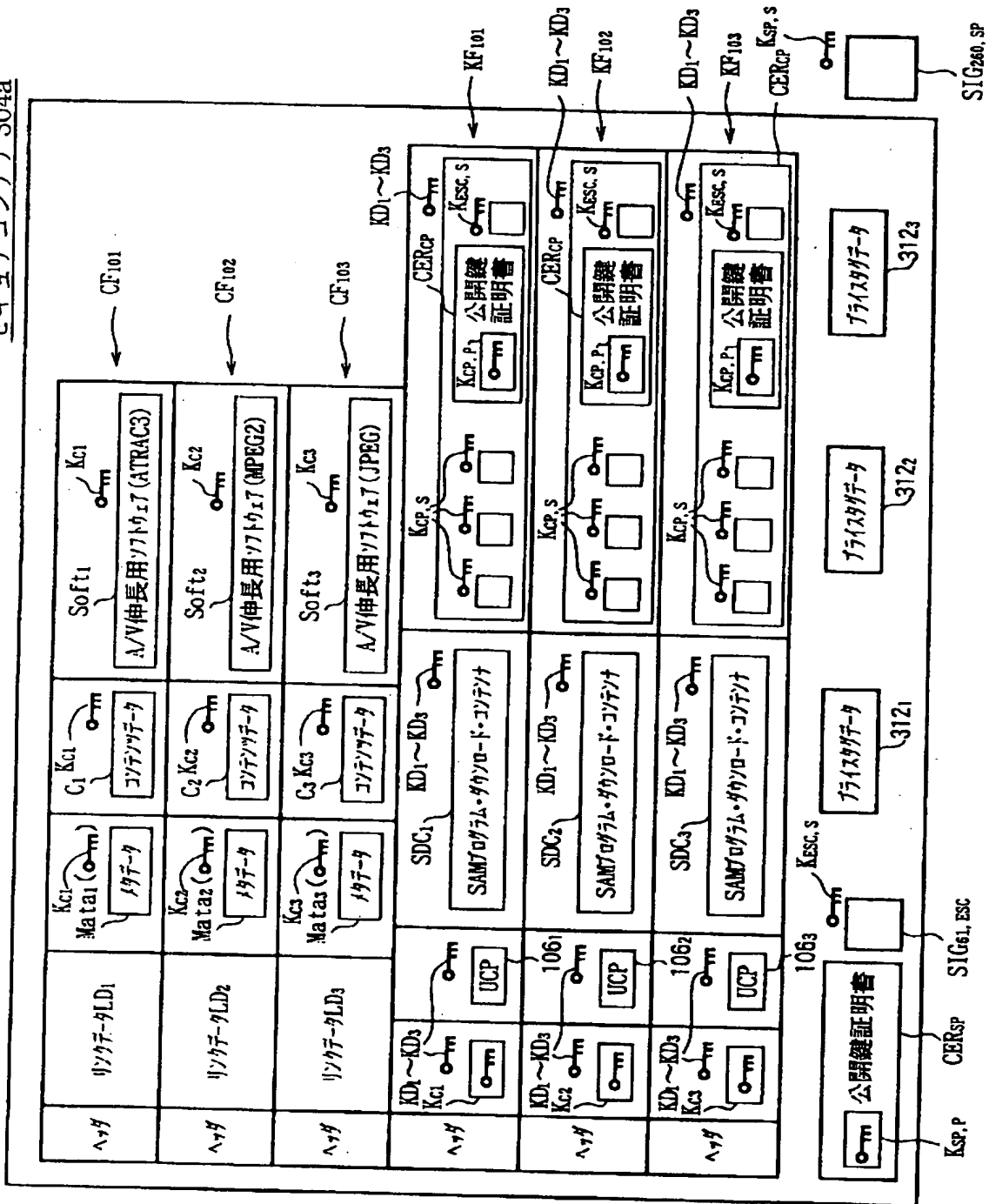


【図 9 4】

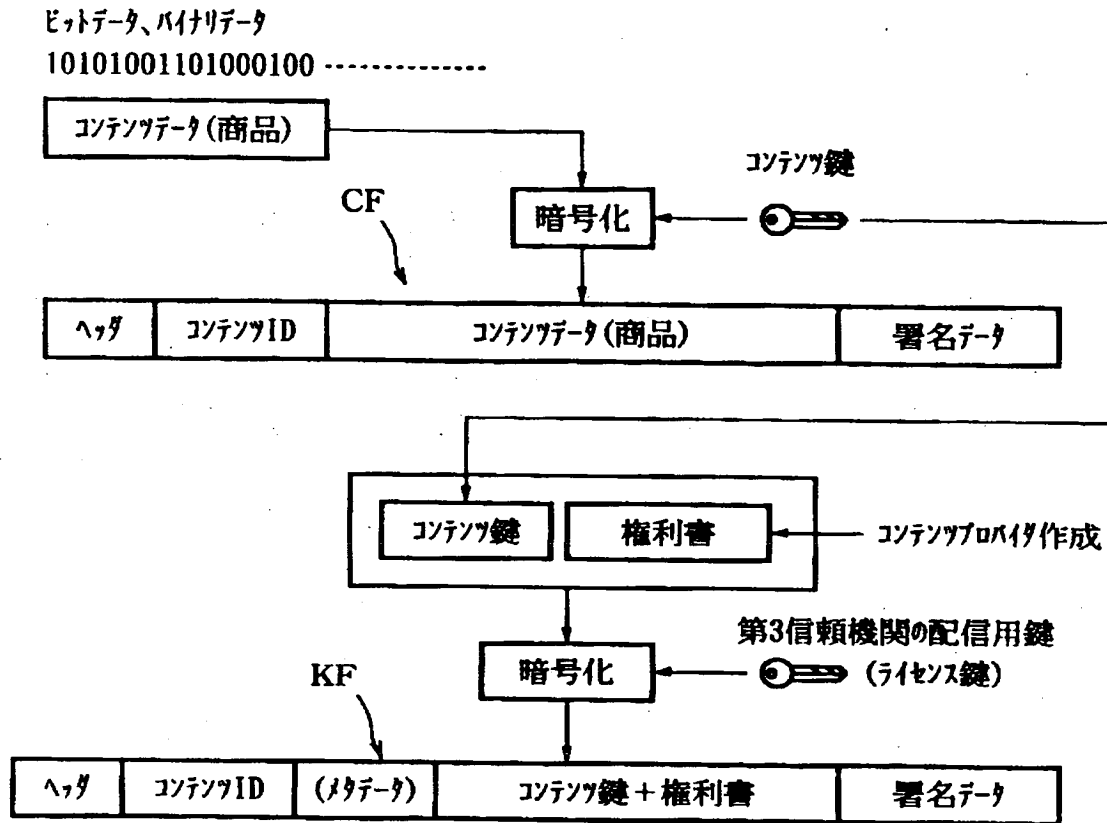


【図 95】

セキュアコンテンツ 304a

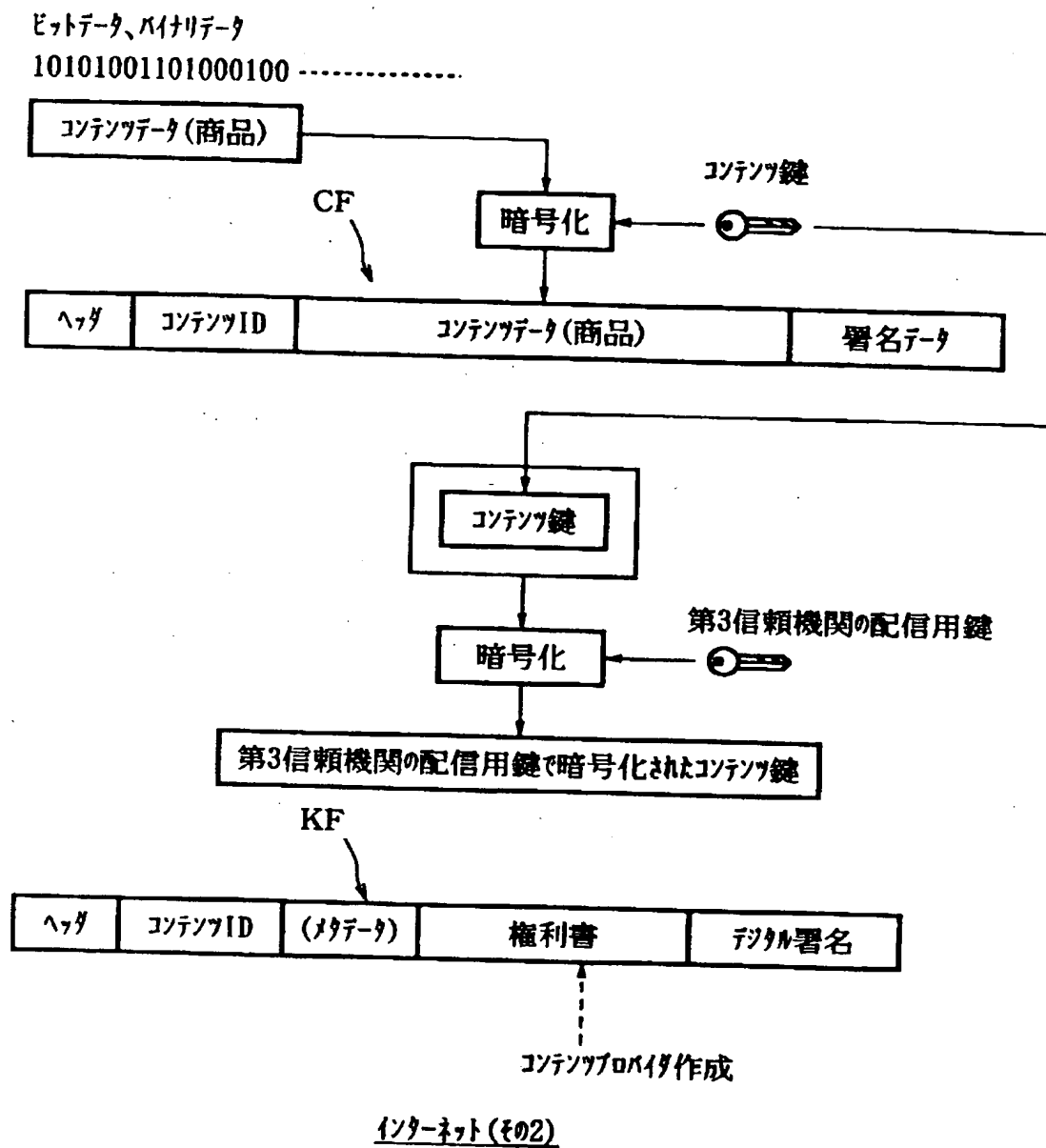


【図 9 6】

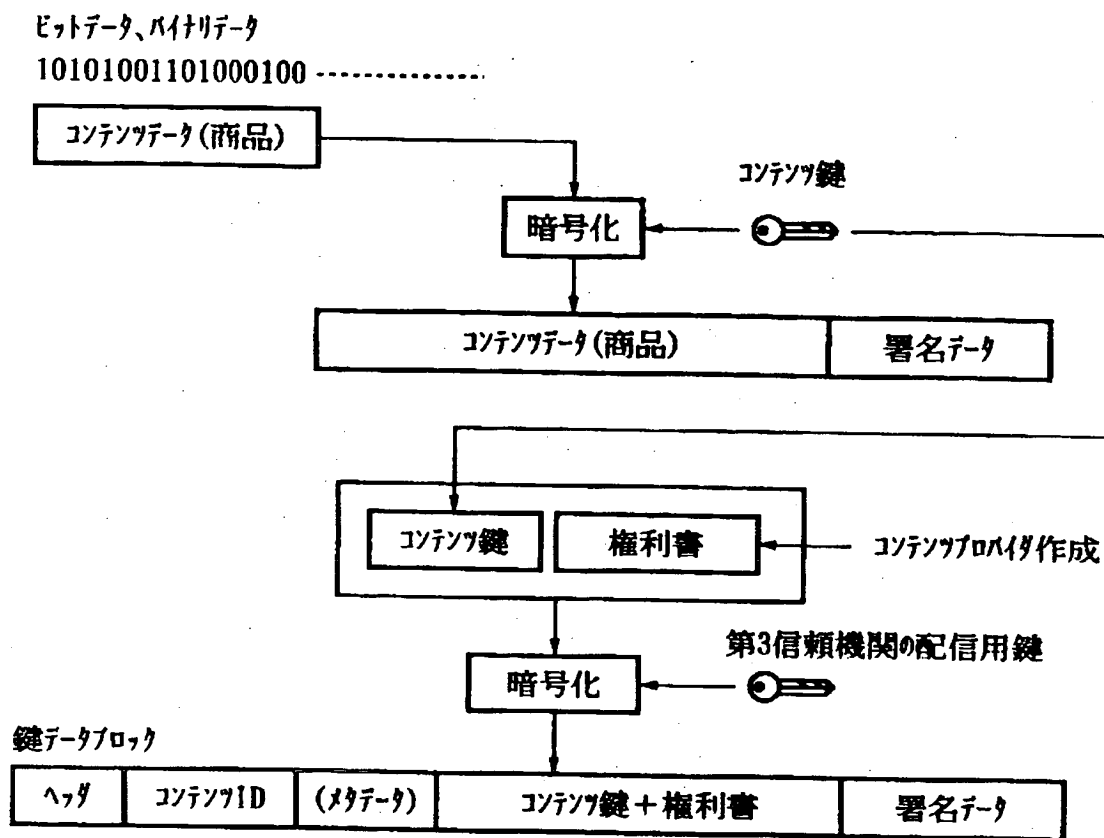


インターネット(その1)

【図 97】

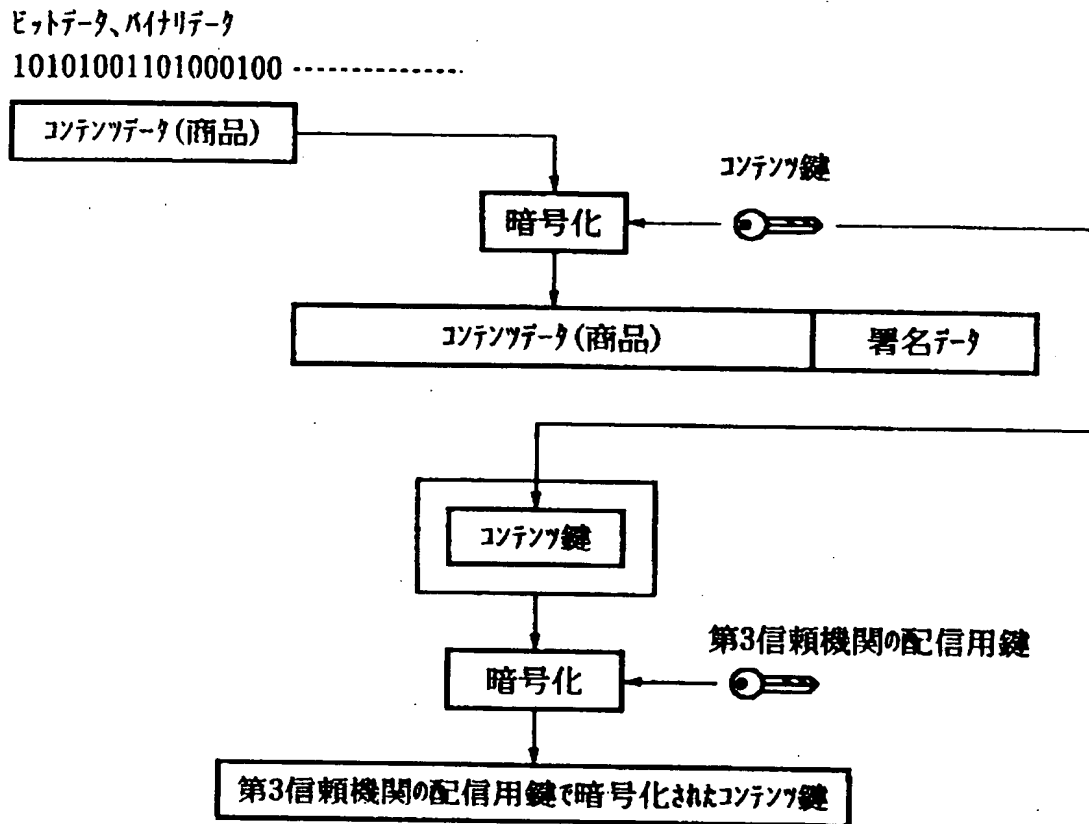


【図 9 8】

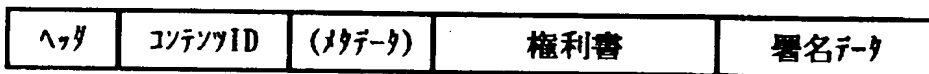


デジタル放送(その1)

【図 99】



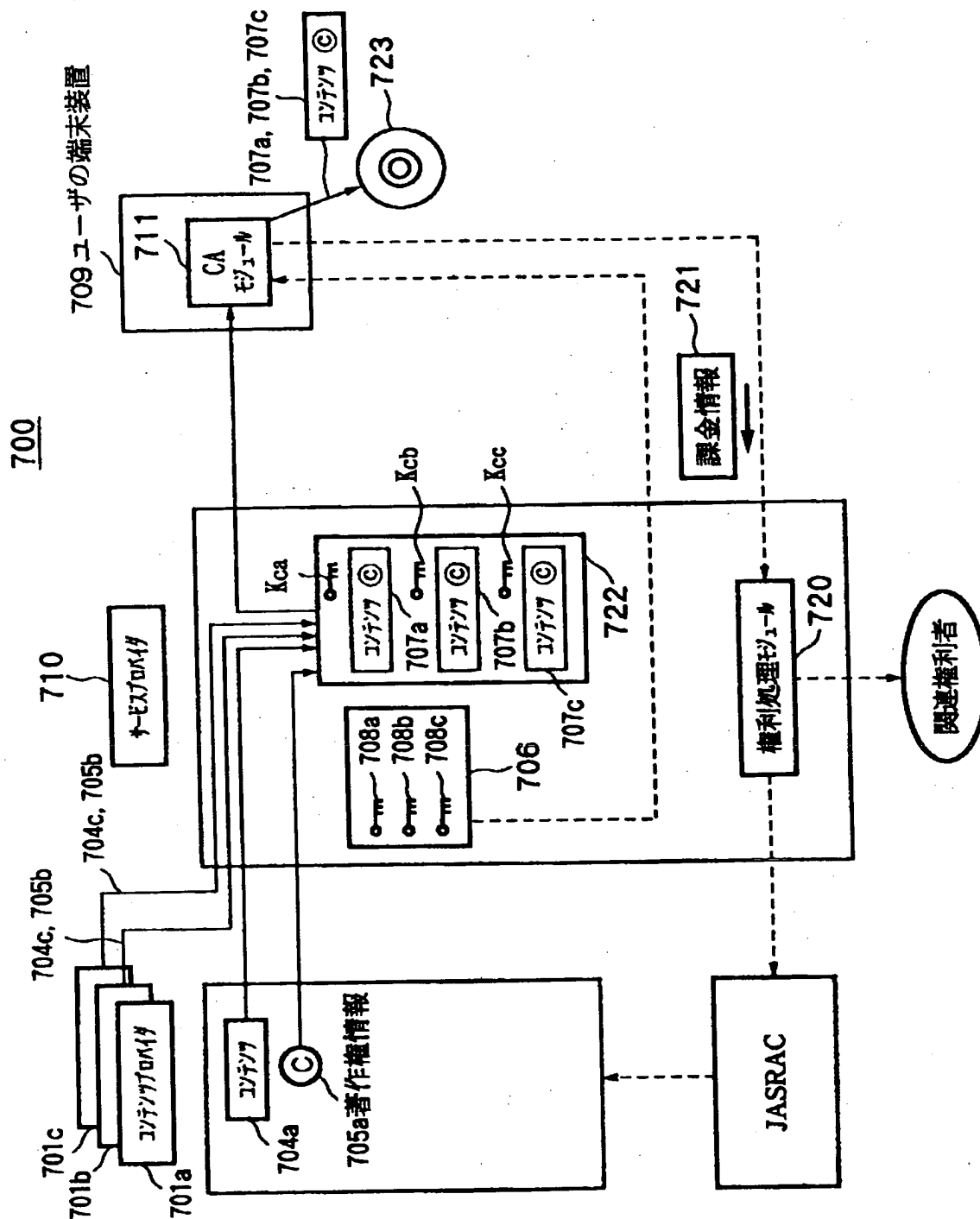
コンテンツ(商品)の取扱方針



コンテンツプロバイダ作成

デジタル放送(その2)

【図100】



【書類名】 要約書

【要約】

【課題】 データ提供装置の関係者の利益を保護できるデータ提供システムを提供する。

【解決手段】 コンテンツプロバイダ 1 0 1 は、コンテンツ鍵データを用いて暗号化されたコンテンツデータと、配信鍵用データを用いて暗号化されたコンテンツ鍵データと、コンテンツデータの取り扱いを示す暗号化された権利書データとを格納したセキュアコンテナ 1 0 4 をユーザホームネットワーク 1 0 3 の S A M 1 0 5₁ などに配給する。S A M 1 0 5₁ などは、セキュアコンテナ 1 0 4 に格納されたコンテンツ鍵データおよび権利書データを復号し、当該復号した権利書データに基づいて、コンテンツデータの購入形態および利用形態などの取り扱いを決定する。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願2000-126305
受付番号	50005028785
書類名	特許願
担当官	第八担当上席 0097
作成日	平成12年 4月26日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000002185
【住所又は居所】	東京都品川区北品川6丁目7番35号
【氏名又は名称】	ソニー株式会社

【代理人】

	申請人
【識別番号】	100094053
【住所又は居所】	東京都台東区柳橋2丁目4番2号 創進国際特許事務所
【氏名又は名称】	佐藤 隆久

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社

THIS PAGE BLANK (USPTO)